Sidang Akhir

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

Oleh:
Febrian Bramanta Alfiansyah
5210 100 087

Dosen Pembimbing I:
Bambang Setiawan, S.Kom, M.T
NIP : 1969 1115 2005 011 003

Dosen Pembimbing II:
Bekti Cahyo Hidayanto, S.Si, M.Kom
NIP : 1975 0405 2008 011 013

Pendahuluan

- Latar Belakang
- Perumusan Masalah
- Tujuan
- Batasan Masalah
- Manfaat

Latar Belakang

- 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.

- 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%

Latar Belakang

- ITS (Institut Teknologi Sepuluh Nopember) sebagai perguruan tinggi yang mengedepankan TI (teknologi informasi) patut mempertimbangkan masalah malware ini.
- Perlunya adanya penelitian untuk mengetahui tren jenis-jenis malware yang ada pada sat ini.

Rumusan Masalah

1. Bagaimana mendapatkan *Autonomous Spreading Malware* dengan menggunakan *Honeypot Dionaea*?
2. Bagaimana melakukan analisis sederhana *Autonomous Spreading Malware* dengan menggunakan *Cuckoo*?

Tujuan

1. Sukses melakukan implementasi *Honeypot Dionaea* dan *Cukoo* pada sebuah komputer di ITS-Net.
2. Melakukan analisis *Autonomous Spreading Malware* agar dapat mengetahui jenis-jenis *malware* yang ada di jaringan ITS-Net.

Batasan Masalah

1. Tools yang digunakan dan berhubungan secara langsung adalah Dionaea dan Cuckoo.
2. Dilakukan analisis sederhana sebagai hasil dari monitoring Autonomous Spreading Malware dengan menggunakan Cuckoo.
3. Studi kasus yang dipakai adalah di pusat kemanan jaringan dan sistem informasi Institut Teknologi Sepuluh Nopember atau yang biasa disebut ITS-Net.

Manfaat

1. Hasil analisis sederhana dapat membantu ITS-Net untuk mengetahui perilaku malware.
2. Informasi data malware dapat digunakan untuk sharing database malware di organisasi/komunitas keamanan internet.

Tinjauan Pustaka

- Malware
- Honeypot
- Dionaea
- Cuckoo

Malware

Malware merupakan singkatan dari *malicious software*, yang artinya perangkat lunak jahat. *Malware* sengaja dibuat oleh penyerang yang bertujuan untuk dapat menginfeksi komputer korban sehingga komputernya dapat dikendalikan oleh si penyerang. *Malware* menginfeksi komputer korban melalui celah keamanan (*vulnerability*) yang ada pada komputer tersebut. Sebagian besar *malware* tersebar melalui jaringan internet. Berdasarkan karakteristiknya, *malware* dapat digolongkan menjadi beberapa jenis yaitu: *worm, trojan, spyware, adware, keylogger, botnet, rootkit* dan *runsomware.*

Honeypot

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

Dionaea

Dionaea merupakan suksesor dari honeypot pendahulunya yaitu nepenthes. Dionaea adalah sebuah low interaction honeypot yang memiliki tujuan untuk mendapatkan copy dari malware. Dionaea dikembangkan menggunakan python sebagai bahasa scripting

Cuckoo

Cuckoo Sandbox merupakan salah satu sistem atau perangkat yang digunakan untuk menganalisis sebuah suspect dalam bentuk malware, atau biasa disebut Malware Analysis Research Toolkit (MART) (10). Cuckoo Sandbox merupakan perangkat yang gratis atau dalam bahasa lain Open Source. Cara kerja dari Cuckoo Sandbox ini adalah dengan memantau segala kejadian yang mungkin di ditimbulkan oleh sebuah malware yang secara sengaja di run di sebuah environtment yang terisolasi.

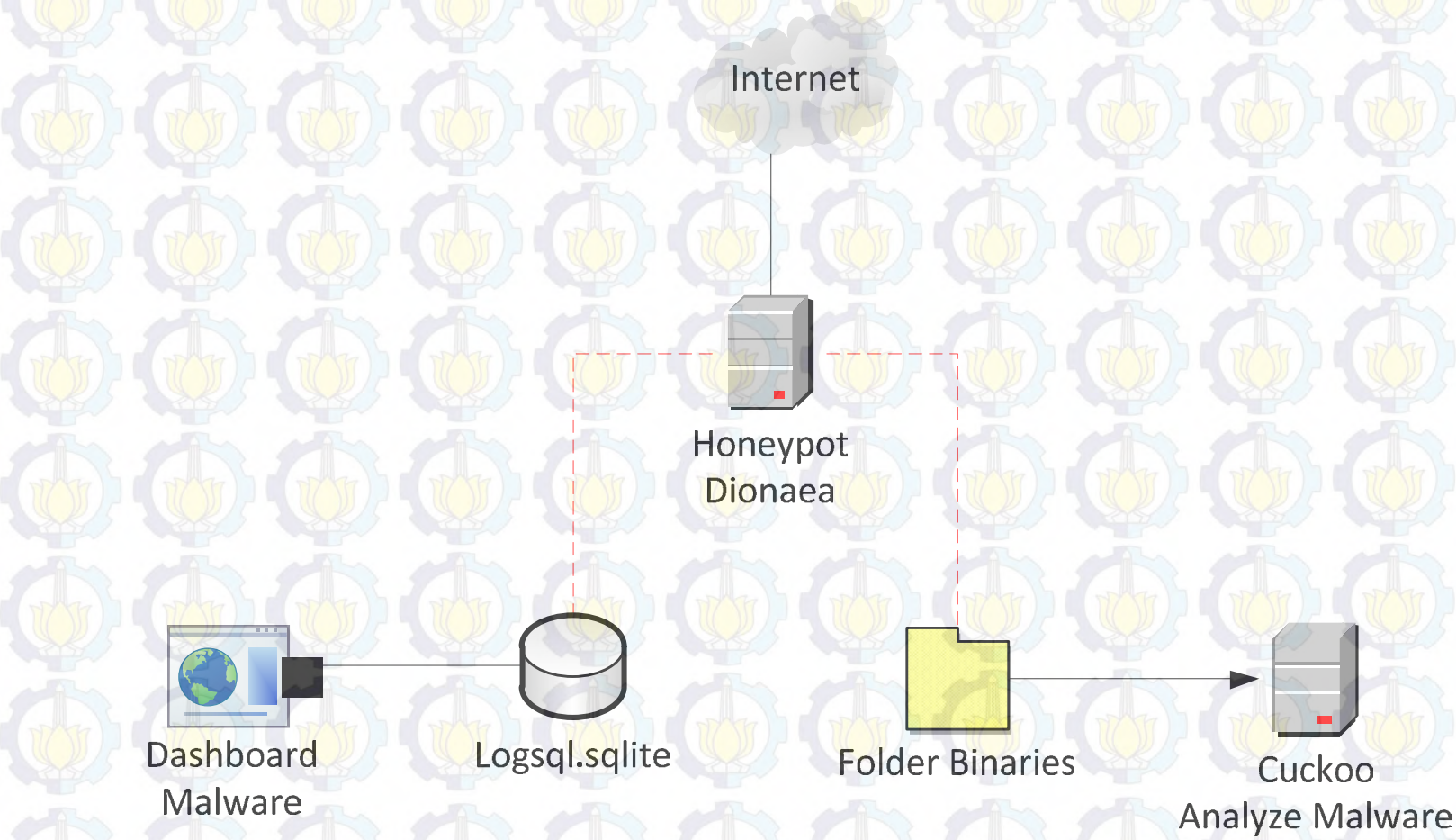
Metodologi

Metodologi

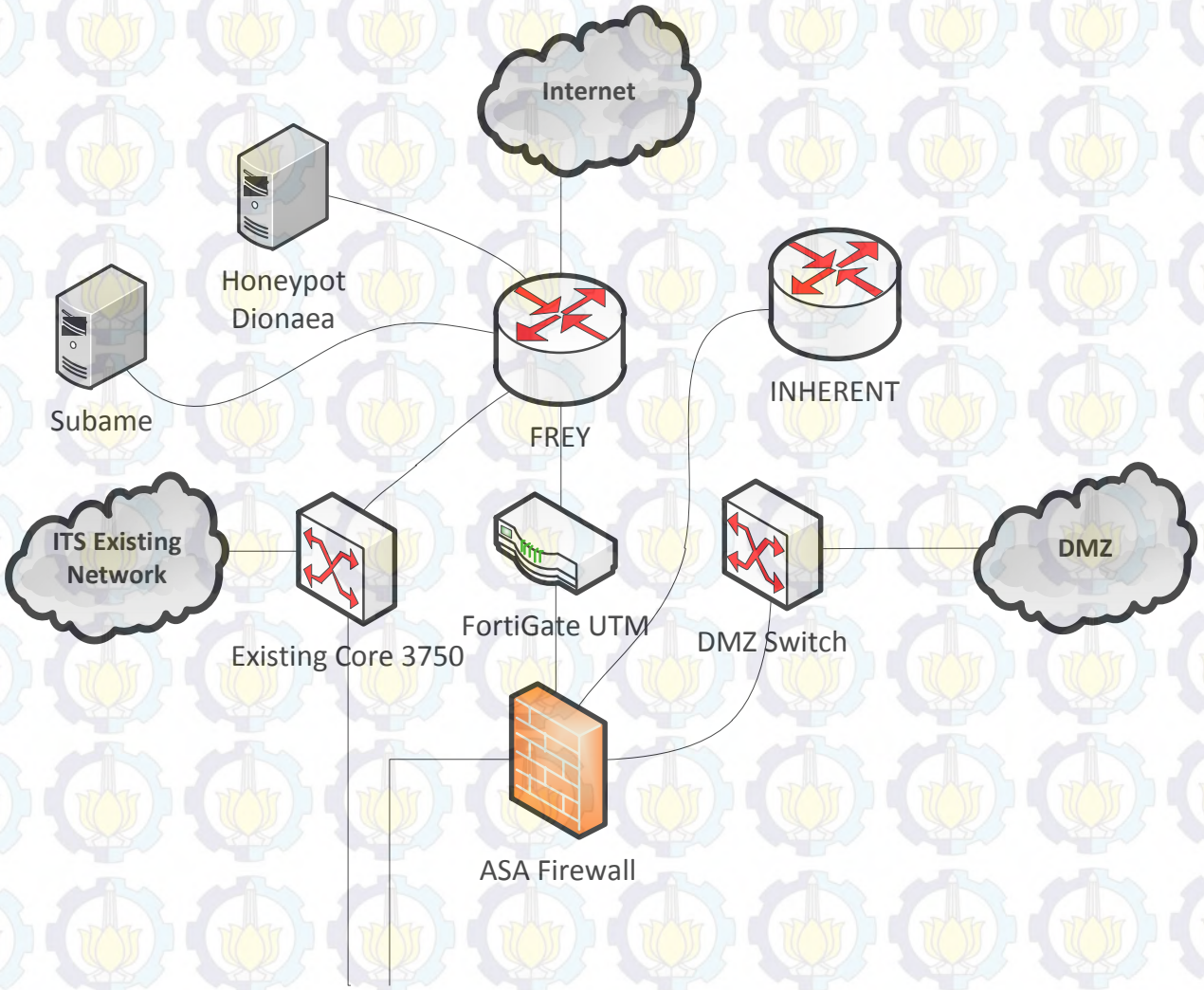

Mulai
Perumusan Masalah dan Penetapan tujuan
Studi Literatur
Perancangan Sistem
Instalasi & Konfigurasi Dionaea dan Cuckoo
Pengambilan Data
Analisis Sederhana
Pembuatan Laporan
Selesai

Perancangan Sistem

Desain Model



Topologi Jaringan



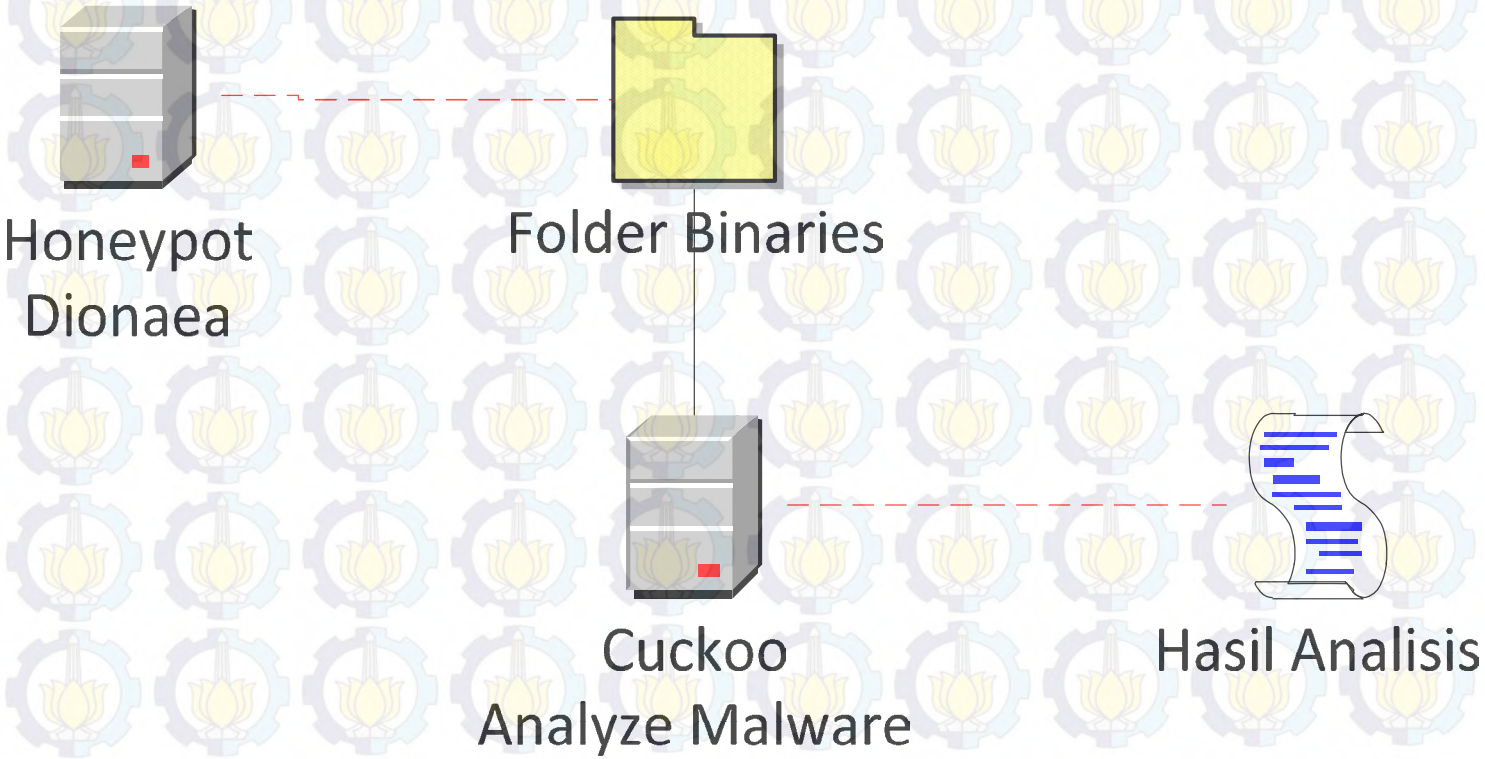
Spesifikasi Hardware

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

Pengambilan Data

1. Dionaea diinstal pada sebuah komputer nano PC
2. Komputer yang telah terinstal Dionaea dipasang di ruang server ITS-Net dengan IP publik kemudian dijalankan
3. Komputer Dionaea akan dijalankan selama 4 bulan untuk memperoleh hasil data malware
4. Pada Dionaea, data log disimpan di dalam database sqlite dengan nama logsql.sqlite. Informasi data yang ada didalamnya akan ditampilkan dalam bentuk web menggunakan DionaeaFR.
5. Malware yang telah ter-download akan tersimpan pada folder "/opt/dionaea/var/dionaea/binaries". Selanjutnya folder binaries akan disalin ke komputer lain dan dilakukan analisis dengan Cuckoo.

Analisis Malware



Analisis Malware

- **Analisis Static**

Pada tahapan analisis static, beberapa informasi yang akan dilihat adalah:

1. Spesifikasi struktur file PE mulai dari package identifier, PE section, imported DLL dan machine type
2. Nama malware berdasarkan signature dari beberapa antivirus
3. Mengidentifikasi jenis file pada malware

- **Analisis Dynamic**

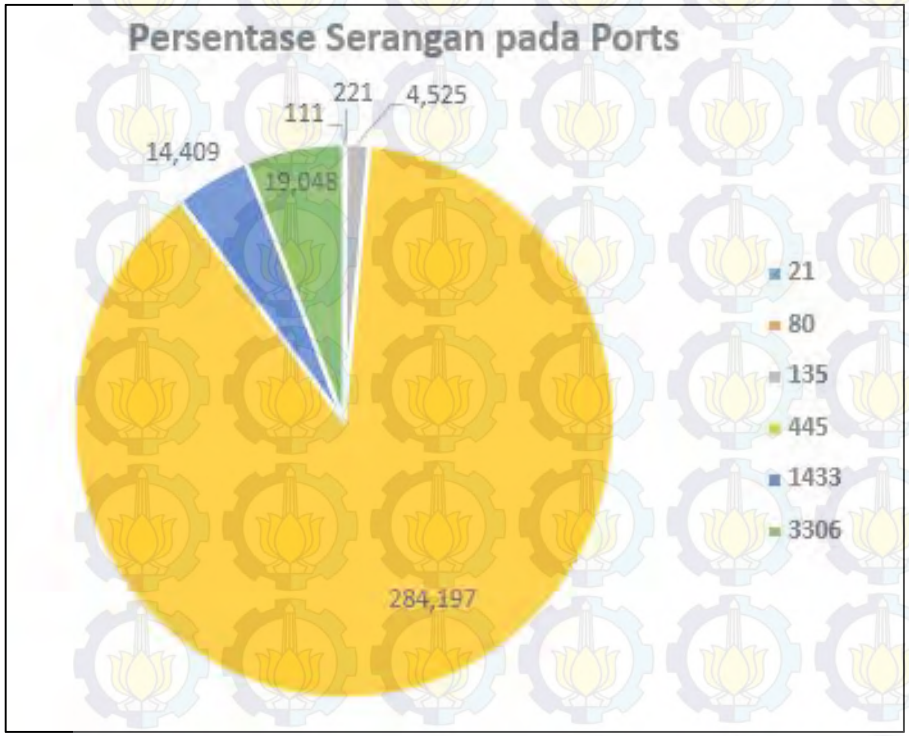
Tujuan dari analisis dynamic adalah untuk melihat aksi dari sebuah malware ketika dieksekusi. Informasi yang akan didapatkan pada saat dilakukan analisis dynamic adalah:

1. File atau folder yang dibuat, dimodifikasi atau dihapus oleh malware
2. Perubahan registry yang muncul akibat malware
3. Koneksi jaringan yang dibuat oleh malware
4. Process yang dijalankan oleh malware

Hasil dan Pembahasan

Hasil Capturing dan Monitoring Malware

- **Jumlah Serangan Berdasarkan Ports**

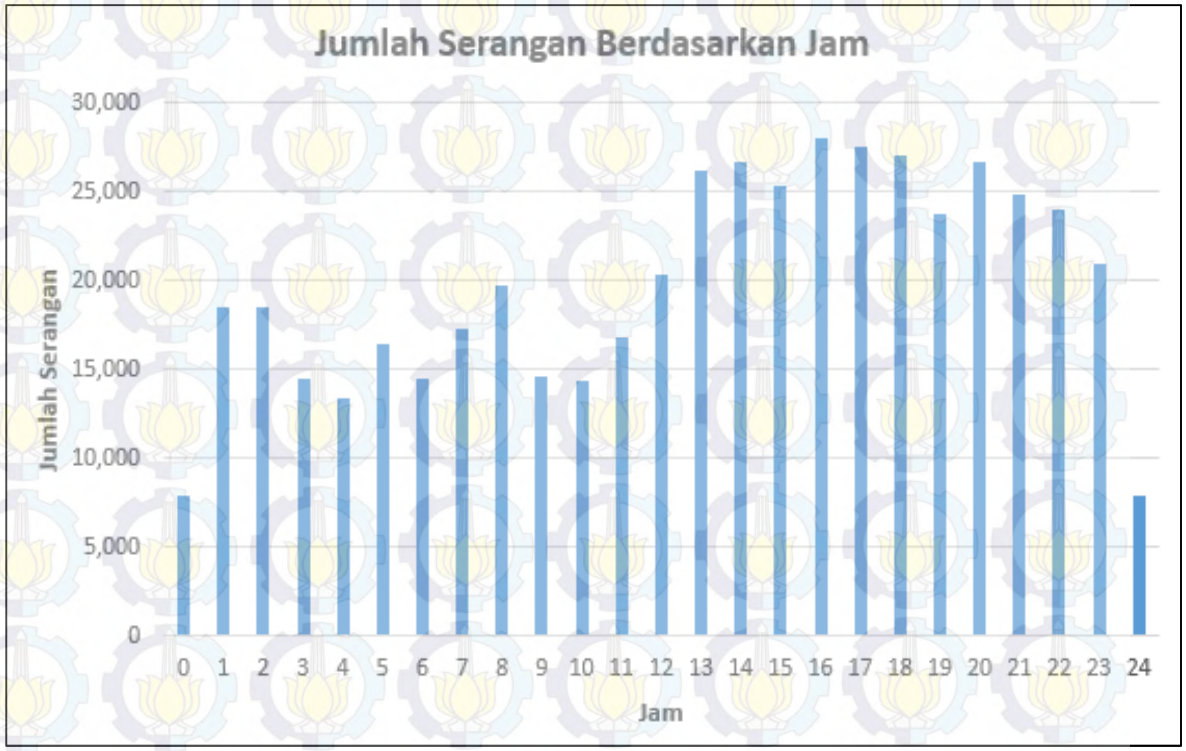


Dari hasil perekaman honeypot Dionaea telah didapatkan informasi port-port berapa saja yang sering digunakan oleh malware untuk melakukan penyerangan. Terdapat 6 port yang menjadi celah untuk masuknya malware, yaitu; 21, 80, 135, 445, 1433 dan 3306. Port 21 adalah port yang digunakan sebagai servis FTP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

Hasil Capturing dan Monitoring Malware

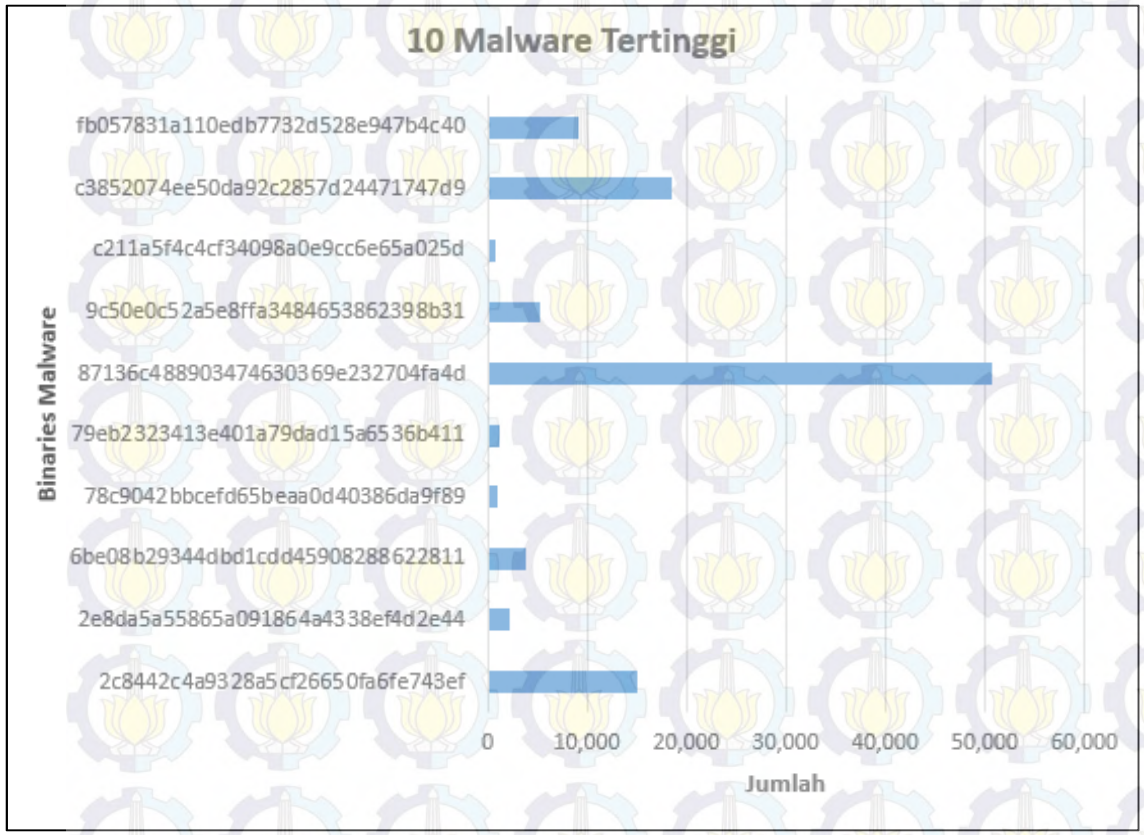
- **Jumlah Serangan Berdasarkan Jam**

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



Hasil Capturing dan Monitoring Malware

- **10 Malware Tertinggi**

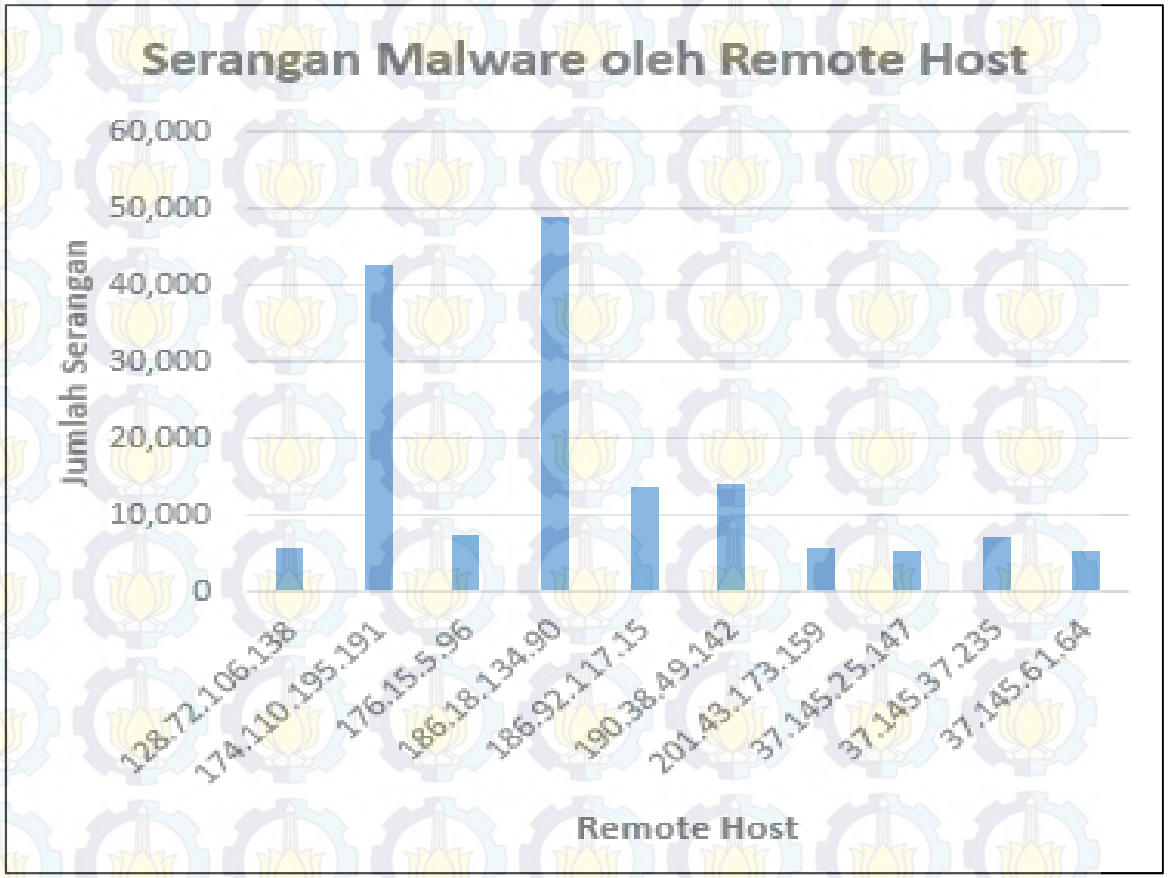


Nama malware yang ditangkap oleh honeypot Dionaea menggunakan format hash MD5 sehingga menghasilkan nama yang panjang dan acak. Dari sekian banyak malware yang berhasil di-download oleh honeypot Dionaea, malware dengan nama 87136c488903474630369e232704fa4d menjadi malware yang paling aktif melakukan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

Hasil Capturing dan Monitoring Malware

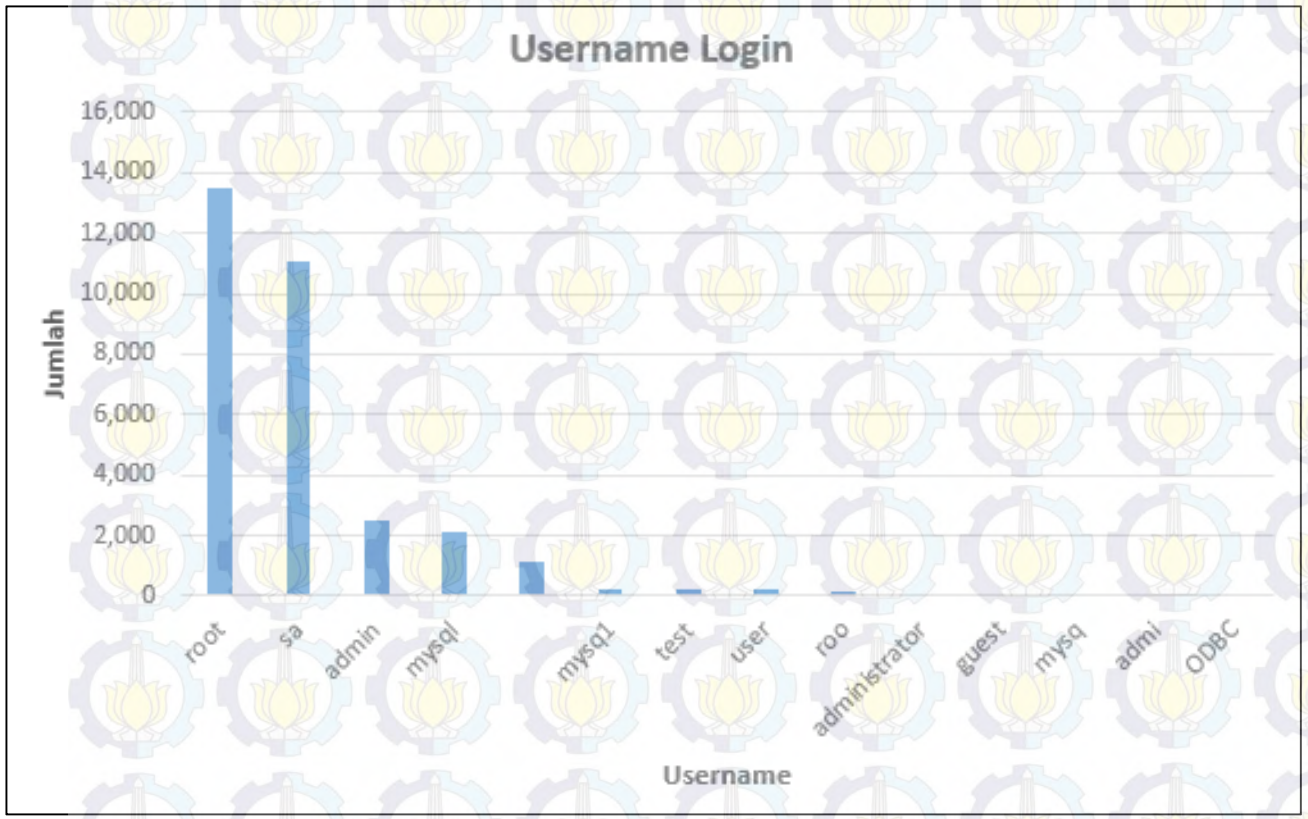
- **Jumlah Serangan Berdasarkan Remote Host**

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.



Hasil Capturing dan Monitoring Malware

- **Jumlah Serangan Berdasarkan Username Login**



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

Analisis Malware dengan Cuckoo

1. 2c8442c4a9328a5cf26650fa6fe743ef

Malware ini dikategorikan sebagai Trojan horse berdasarkan dari hasil scanning signature antivirus Avast dan Avira. Malware ini melakukan request koneksi ke IP 74.125.224.53 dan hasil tracing menunjukkan bahwa IP tersebut merupakan milik host gmail.com. Pembuat malware biasanya melakukan enkripsi pada kompresi malware sehingga sulit untuk dideteksi, namun malware ini dapat dideteksi menggunakan tools packer bernama Armadillo.

2. 2e8da5a55865a091864a4338ef4d2e44

Malware ini dikategorikan sebagai spyware yang bekerja dengan mengumpulkan informasi pribadi dengan cara merubah registry, cookies, history dan cache.

Analisis Malware dengan Cuckoo

3. 6be08b29344dbd1cdd45908288622811

Malware ini dikategorikan sebagai Rbot atau Spybot. Behavior analisis untuk malware ini taidak didapatkan karena Cuckoo gagal melakukan analisis untuk malware ini

4. 78c9042bbcefd65beaa0d40386da9f89

Malaware ini dikategorikan sebagai Trojan. Trojan melakukan infeksi pada komputer dengan cara membuat backdoor dan penyerang akan melakukan remote pada komputer melalui backdoor ini. Malware ini membuat file explorer.exe palsu yang digunakan untuk memasukkan file desktop.ini dan ecleaner.exe ke dalam sistem.

5. 79eb2323413e401a79dad15a6536b411

Malware ini dikategorikan sebagai Worm. Hasil analisis behavior menunjukkan malware mencoba malakukan distribusi file ke 5219 alamat IP dibawah subnet 81.88.0.0

Analisis Malware dengan Cuckoo

6. 87136c4889034746303 69e232704fa4d

Malware ini dikategorikan sebagai Trojan. Tugas dari malware yaitu melakukan koneksi dengan host d.homler.net yang memiliki alamat IP 117.21.224.29. Malware membuat 2 remote threads yaitu explorer.exe dan wuauclt.exe.

7. 9c50e0c52a5e8ffa348465386 2398b31

Malware ini dikategorikan sebagai Worm. Ketika malware ini berjalan akan melakukan penghapusan service dengan nama urdvxc.exe.

8. c211a5f4c4cf34098a0e9cc6e65a025d

Malware ini dikategorikan sebagai Trojan. Malware melakukan perubahan pada registry dengan memasukkan nilai baru ke dalam “HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\” untuk menjalankan ecleaner pada saat Windows startup.

Analisis Malware dengan Cuckoo

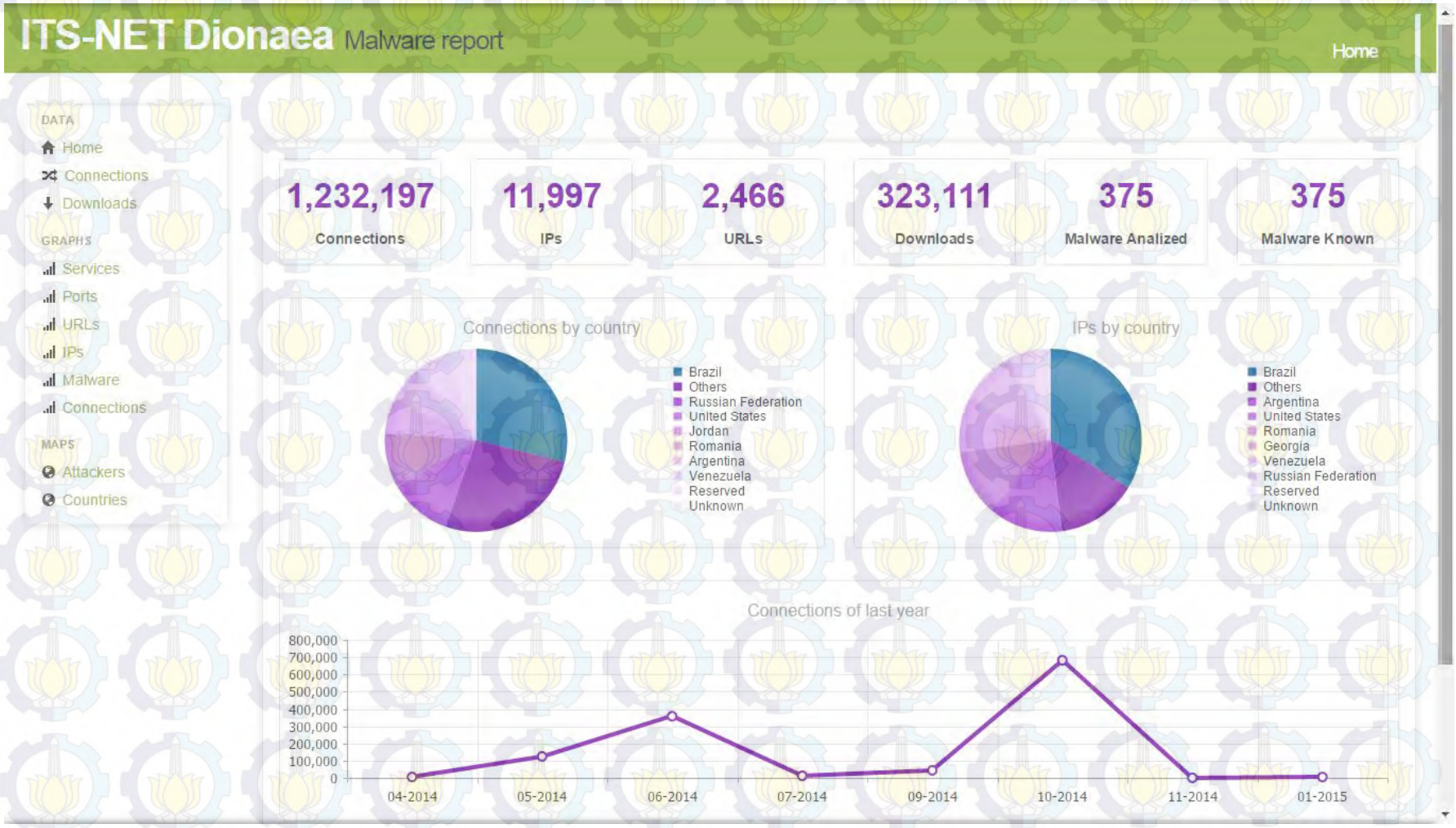
9. c3852074ee50da92c2857d24471747d9

Malware ini dikategorikan sebagai Worm. Dari hasil analisis di Cuckoo menunjukkan aktifitas malware di jaringan dengan membuat koneksi scan UDP pada subnet 67.138.0.0.

10. fb057831a110edb7732d528e947b4c40

Malware ini dikaegorikan sebagai IRC bot. Aktifitas malware melakukan perubahan registry dan file. Pertama malware membuat file gwind.exe yang selalu berjalan ketika windows startup yang berfungsi untuk men-disable proxy internet explorer. Selanjutnya malware akan melakukan komunikasi dengan host tv.homlet.net.

Dashboard Malware



Kesimpulan dan Saran

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 analisis *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%.

Saran

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.

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

Terima Kasih