Faktor Exacta 12(2): 145-155, 2019
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI : 10.30998/faktorexacta.v12i2.3549

Menelaah Lalu Lintas Jaringan Internet Relay Chat (IRC) Yang Berbahaya guna Identifikasi Komunikasi *Botnet* "Plague"

SURYO BRAMASTO
Program Studi Informatika
Institut Teknologi Indonesia
Jalan Raya Puspiptek Serpong, Kota Tangerang Selatan, Banten-15320
Tlp: +62217561102, +6281563470055
E-mail: suryo.bramasto@iti.ac.id

Abstract. *The research presented in this article aims to identify "plague" botnet communication pattern, with the aid of Wireshark Packet Analyzer as proof of concept (PoC) towards unique communication pattern analysis between infected host and botnet. The research is conducted on public IRC (Internet Relay Chat) network, specifically at the opened domain for botnet research, that is, irc.accesox.net. COMODO Internet Security also used for determining files downloaded by the botnet to identify whether there any malware or not. The observation is done on 60 captured packets, which then the TCP stream excerpt and the protocols hierarchy statistic from those packets being analyzed. Based on the analysis of TCP stream excerpt and the protocols hierarchy statistic, the communication pattern between bot, botmaster, and infected host are known. Wireshark could show the data inside the TCP stream excerpt and all captured protocols. The conducted analysis on TCP stream excerpt and protocols hierarchy statistic is based on RFC 2812 (Internet Relay Chat: Client Protocol – IETF Tools). The analysis on TCP stream excerpt and protocols hierarchy statistic yield botnet activity information for the next step of the analysis of botnet attack, which is dataset and prediction model building. The prediction model can then be implemented to predict whether network traffic is safe or harmful.*

Keywords: botnet, COMODO internet security, Internet Relay Chat (IRC), RFC 2812, Wireshark

Abstrak. Penelitian yang disajikan pada artikel ini bertujuan mengidentifikasi pola komunikasi botnet *"plague"* dengan bantuan *Wireshark Packet Analyzer* untuk menunjukkan *proof of concept* (PoC) analisis pola komunikasi unik antara *host* terinfeksi dengan botnet. Penelitian dilakukan terhadap jaringan IRC (*Internet Relay Chat*) publik, yaitu pada domain yang secara spesifik dibuka guna melakukan penelitian terkait *botnet* yaitu domain irc.accesox.net. Digunakan juga COMODO Internet Security guna melakukan pemeriksaan terhadap *file-file* yang diunduh oleh botnet, apakah merupakan file yang berbahaya (*malware*) atau tidak. Penelitian dilakukan dengan melakukan observasi terhadap 60 paket tertangkap, selanjutnya dilakukan analisis terhadap *excerpt* dari aliran TCP berikut statistik hirarki protokol pada paket-paket tertangkap. Berdasarkan analisis terhadap pembacaan *excerpt* dari aliran TCP, serta hirarki protokol tertangkap berikut data di dalamnya maka dapat diketahui pola komunikasi antara *bot, bot master*, dan *infected host*. Analisis terhadap hasil pembacaan dilakukan sesuai pemahaman dari RFC 2812 (Internet Relay Chat: Client Protocol – IETF Tools). Wireshark mampu menampilkan komunikasi antara *bot, bot master*, dan *infected host* dengan cukup jelas, dan dengan pemahaman terhadap RFC 2812, maka dapat diperoleh informasi aktivitas *botnet* guna proses kelanjutan dari analisis serangan *botnet* yakni membangun *dataset* dan model prediksi, yang mana kemudian model tersebut dapat diimplementasikan guna memprediksi apakah suatu lalu-lintas jaringan aman atau berbahaya.

Kata kunci: botnet, COMODO Internet Security, Internet Relay Chat (IRC), RFC 2812, Wireshark

Faktor Exacta *12 (2):* 145-155, 2019
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI : 10.30998/faktorexacta.v12i2.3549

PENDAHULUAN

Botnet dalam domain keamanan informasi, *digital forensics*, dan respon insiden, sering dikaitkan sebagai mekanisme inang dari data ilegal, peluncuran serangan DDOS (Distributed Denial of Services), pencurian informasi, *spamming*, bitcoin *mining*, penyebaran *ransomware*, peluncuran serangan *brute force*, mengelola akses jarak jauh terhadap perangkat-perangkat terkoneksi, propagasi infeksi ke perangkat lain, dan sebagainya. Jaringan-jaringan Internet Relay Chat (IRC) merupakan media yang populer guna pengendalian jaringan-jaringan *bot*. *Bot-bot* berbasis IRC dengan berbagai derajat kerumitan serta dengan struktur perintah yang berbeda-beda memiliki kesamaan pada suatu hal. Sebuah bot IRC, saat dieksekusi pada mesin client, maka akan terhubung ke server IRC pada *port-port* acak dengan nomor-nomor *port* besar, *logs* ke dalam kanal yang sudah ditentukan sebelumnya secara pasti, serta kemudian mendengarkan perintah-perintah dari *bot master*.

Daur hidup *botnet* dimulai dengan fase infeksi, dimana suatu sistem diserang oleh preconfigured *customized malware*. Fase koneksi adalah saat sistem terinfeksi melakukan inisiasi hubungan pada IRC TCP service port yang sudah ditentukan guna komunikasi secara *remote*. Akses *bot* ke kanal komunikasi dimungkinkan terotentikasi menggunakan *username, nickname, password*, atau *key*. Pada fase perintah dan kendali, *bot* menerima perintah dari *bot master* melalui kanal komunikasi/*channel for communication* (C2C) tertentu. Akhirnya pada fase penggandaan, *preconfigured customized malware* didownload ke dalam bot terinfeksi untuk pengendalian lebih lanjut dan penyebaran infeksi melalui perangkat penyimpan seperti USB *flash drive* dan semacamnya, atau penyebaran infeksi melalui jaringan komputer terkonfigurasi *shared writable*.

Menurut Alothman dan Rattadilok (2017), deteksi *botnet* merupakan salah satu area penelitian aktif selama sepuluh tahun terakhir, dimana para peneliti berusaha keras mengembangkan teknik-teknik yang efektif guna mendeteksi *botnet*. Mulai dari *review* terhadap pendekatan-pendekatan yang telah ada terhadap *botnet-botnet* spesifik, hingga mencoba mengidentifikasi aktivitas *botnet* dengan melakukan analisis terhadap lalu lintas jaringan. Artikel ini bertujuan untuk menunjukkan sebuah *proof of concept* (PoC), yang ditujukan guna melakukan analisis terhadap pola komunikasi unik antara *host* terinfeksi dengan *botnet*. Analisis digunakan dengan alat bantu Wireshark. Analisis dan observasi akan membantu investigasi awal dari identifikasi lalu lintas pada jaringan tercuplik tentang perilaku *bot* seperti bagaimana *bot* masuk ke sebuah kanal, pertukaran pesan antara *bot* dengan *bot master*, penyebaran infeksi, dan sebagainya. PoC ini akan merumuskan informasi-informasi guna tahap berikutnya dari analisis serangan *botnet* yakni proses *data analytic* guna deteksi *botnet*.

Landasan Teori

Botnet

Menurut Ramneek Puri (2003), *botnet* adalah sekumpulan program yang saling terhubung melalui internet, yang berkomunikasi dengan program-program sejenis untuk melakukan tugas tertentu. *Botnet* bisa dipakai untuk menjaga keamanan kanal IRC, mengirimkan *spam* e-mail, atau berpartisipasi dalam serangan DDoS. Kata *botnet* berasal dari kata robot dan *network*.
Botnet dieksploitasi untuk berbagai keperluan, antara lain serangan DoS, penciptaan atau penyalahgunaan relai surat SMTP untuk *spam* (*Spambot*), pemalsuan klik, *spamdex*, pencurian nomor serial aplikasi, identitas masuk *log*, dan informasi keuangan seperti nomor kartu kredit.
Komunitas pengendali *botnet* sudah lama berjuang memperebutkan gelar pemilik bot terbanyak, konsumsi *bandwidth tertinggi*, dan mesin terinfeksi paling "berkepentingan tinggi", seperti universitas, perusahaan, dan pemerintahan.

Contoh Operasi *Botnet*

Ilustrasi contoh operasi *botnet* guna pengiriman spam e-mail ditunjukkan pada gambar 1.

Faktor Exacta *12 (2):* 145-155, 2019
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI : 10.30998/faktorexacta.v12i2.3549

Gambar 1. Operasi Botnet untuk Pengiriman *Spam E-mail*

Tahapan operasi *botnet* guna pengiriman *spam* e-mail adalah sebagai berikut:

1. Operator *botnet* menyebarkan virus atau *worm* yang menginfeksi komputer pengguna biasa dengan perantara aplikasi bot.
2. *Bot* di Personal Computer (PC) yang terinfeksi *log* ke *server C&C* (*command & control*) tertentu.
3. Seorang *spammer* membeli jasa *botnet* dari operator.
4. *Spammer* menyampaikan pesan *spam* kepada operator. Operator menginstruksikan mesin terinfeksi untuk mengirimkan pesan *spam* melalui panel kendali pada server *web*.

Ancaman *Cyber* Berbasis *Botnet*

Kasperzyk, Paz, dan Tarapata (2017) menyatakan bahwa dengan melakukan analisis terhadap data historis, dapat diketahui bahwa mayoritas kasus serangan *botnet* adalah *zombies* atau *bots* yang terinfeksi *malware*. Kemudian berdasarkan penelitian oleh Vitaly Kamluk (2008) yang disitasi oleh Kasperzyk, Paz, dan Tarapata (2017), menyatakan bahwa botnet dapat memberikan pembuatnya derajat tertentu terhadap kendali perangkat yang diserang. Apa yang terjadi pada sejumlah komputer yang terinfeksi *botnet* tertentu, biasanya berbeda atau bahkan sangat berbeda dibandingkan dengan apa yang terjadi karena jenis *bot* yang lain. Sejumlah *bot* mampu melakukan banyak serangan tanpa diketahui oleh pengguna perangkat atau *domain* yang diserang. Begitupula kemudahan dan biaya pengelolaan *botnet* yang rendah semakin meningkatkan popularitas *botnet.* Sfakianakis et al (2018) merilis daftar aktivitas *botnet* di seluruh dunia, yang ditunjukkan pada tabel 1.

Faktor Exacta *12 (2):* 145-155, 2019
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI : 10.30998/faktorexacta.v12i2.3549

Tabel 1. Daftar Aktivitas *Botnet* pada 2018

No.	Botnet name	No. of IP addresses	Percentage
1	*Conficker*	62 221	21.19%
2	*ZeroAccess*	32 460	11.57%
3	*Zeus (incl Citadel)*	25 311	9.03%
4	*Sality*	14 003	4.99%
5	*Zeus GameOver*	12 513	4.46%
6	*Ircbot*	10 768	3.84%
7	*Bankpatch*	6 086	2.17%
8	*Banatrix*	5 385	1.92%
9	*Virut*	4 014	1.43%
10	*Kelihos*	3 922	1.40%
	Other	103 750	37.00%

Berdasarkan penelitian yang dilakukan Godkin T. (2013) yang disitasi oleh Kasperzyk, Paz, dan Tarapata (2017), *botnet* juga telah menjadi sumber pemasukan bagi kelompok-kelompok *cybercriminal* besar, seperti misalnya "DNSChanger", yang menggunakan empat juta *bot* guna menginjeksikan iklan, menghasilkan 14 juta USD selama lima tahun beroperasi. Begitupula "Storm", yang menggunakan 3,5 juta *bot* guna *spamming*, menghasilkan sekitar 3,5 juta USD per tahun. Ancaman berikutnya yakni bahwa resiko terhadap serangan berbasis *botnet* meningkat secara signifikan karena jaringan *botnet* guna serangan *cyber* dapat dibeli seperti berikut:

1) *Botnet* guna serangan DDoS 24 jam: 30 – 70 USD
2) *Botnet* guna spam email: 10 USD per 1 juta email spam
3) Pembelian 1 paket berisi 2000 *bot*: 200 USD
4) 1 paket berisi *bot-bot* yang mampu melakukan serangan DDoS secara efisien: 700 USD

Packet Analyzer

Packet Analyzer (Packet *Sniffer*) merupakan perangkat lunak atau perangkat keras yang mampu mencegat (*intercept*) dan mencatat (*log*) bagian atau keseluruhan lalu lintas jaringan digital. Proses *intercepting* dan *l*ogging disebut dengan *packet capture*. Selama aliran data mengalir pada jaringan komputer, Sniffer menangkap setiap paket, dan jika diperlukan melakukan *decoding* terhadap *raw data* dari paket sehingga menunjukkan nilai-nilai pada berbagai *field* dari paket, serta menganalisis isi paket sesuai spesifikasi yang dibutuhkan. Terdapat juga Packet Analyzer untuk jaringan nirkabel (*Wireless/WiFi Analyzer*).

Kapabilitas Packet *Analyzer*

Pada jaringan kabel seperti Ethernet, Token Ring, dan FDDI, dimungkinkan untuk menangkap keseluruhan lalu lintas jaringan dari setiap mesin pada jaringan komputer tersebut (tergantung struktur *hub* atau *switch*nya). Pada jaringan modern (kombinasi), lalu lintas dapat ditangkap melalui monitoring *port* pada *network switch* atau menggunakan *network tap* yang lebih handal saat lalu lintas jaringan sibuk. Pada lalu lintas nirkabel, penangkapan dapat dilakukan pada satu demi satu kanal atau beberapa kanal sekaligus menggunakan lebih dari satu adapter.

Pada mode *broadcast* berbasis kabel, guna menangkap lalu lintas *unicast* antar mesin, *network adapter* yang digunakan untuk penangkapan harus dalam mode *promiscuous*. Sedangkan pada mode *broadcast* nirkabel, agar dapat dilakukan penangkapan maka *network adapter* harus berada dalam mode monitor.

Saat lalu lintas ditangkap, keseluruhan isi paket direkam, atau dapat juga hanya pada bagian header saja yang direkam guna mengurangi kebutuhan penyimpanan. Namun jika hanya bagian header saja yang direkam dapat mengakibatkan kurangnya informasi guna keperluan diagnosis permasalahan.

Faktor Exacta *12 (2):* 145-155, 2019
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI : 10.30998/faktorexacta.v12i2.3549

Setelah informasi tertangkap, maka dilakukan decoding terhadap informasi tersebut dari format *raw* digital ke format yang terbaca manusia. Packet Analyzer pada umumnya juga memiliki fitur *protocol analyzer*, yang memungkinkan untuk menampilkan data secara berganda, deteksi error otomatis, menentukan akar terjadinya error, menghasilkan timing diagram, rekonstruksi aliran data TCP dan UDP, berlaku sebagai *reference device* dengan menghasilkan lalu lintas dan sebagainya.

METODE

Observasi dan Penyimpulan Pola Komunikasi

Dilakukan observasi terhadap 60 paket, yang kemudian tersimpan sebagai file .pcap. Dari hasil observasi dilakukan penyimpulan pola komunikasi IRC. Penyimpulan ini mengkelompokkan pola komunikasi normal dan pola komunikasi *bot* yang berbahaya berdasar ada atau tidaknya *malware* yang terlibat.

Analisis

Selanjutnya dilakukan analisis terhadap hasil observasi dan penyimpulan pola komunikasi, yakni yang pertama adalah analisis terhadap properti-properti file .pcap menggunakan Wireshark. Yang kedua adalah analisis terhadap TCP Stream juga menggunakan Wireshark guna memperoleh informasi yang relevan guna lebih memahami komunikasi *bot*. Yang ketiga yakni analisis hirarki protokol, karena pada umumnya paket-paket mengandung beberapa protokol, dimana juga dilakukan dengan alat bantu Wireshark. Sedangkan proses berikutnya atau yang ketiga adalah analisis terhadap statistik hirarki protokol, yang mana Wireshark mampu menampilkan data dalam semua protokol tercuplik, yang ditampilkan secara hirarkis. Proses analisis dengan alat bantu Wireshark ini mengacu kepada panduan yang dirumuskan oleh Graham Bloice (2019).

Observasi

Proses observasi dijabarkan sebagai berikut:

1. Secara keseluruhan, terdapat 60 paket yang diobservasi. Identifikasi alamat Internet Protocol (IP) dari paket-paket tersebut yakni:
   1) 192.168.45.130: port 1037 (service: ams); port 1038 (service: mtqp)
   2) 192.168.45.2: port 53 (service: DNS)
   3) 91.121.100.60: Resolved Address- irc.accesox.net; TCP port 5540 (service: sdreport)
2. IP 192.168.45.130: 1037 menginisiasi sebuah *query* DNS ke 192.168.45.2:53 untuk *name resolution* dari irc.accesox.net. Respon DNS dari 192.168.45.2 pada 91.121.100.60 dan 91.121.96.162.
3. Paket, 3, 4, dan 5 berisi detail TCP three-way handshake. *Handshake* tersebut diinisiasi dari 192.168.45.130:1038 dan ditujukan ke irc.accesox.net (91.121.100.60:5540).
4. Paket 6 berisi pesan IRC “PASS” yang digunakan untuk memasang sebuah “password koneksi” oleh *host bot* 192.168.45.130. “Password koneksi” ini digunakan untuk registrasi koneksi dengan server IRC irc.accesox.net (91.121.100.60).
5. Paket 8 berisi pesan IRC “NICK” yang digunakan untuk menyediakan sebuah username yakni “pLagUe{“ oleh *host* 192.168.45.130.
6. Paket 10 berisi pesan IRC “USER” yang digunakan untuk menetapkan *username* oleh *host* 192.168.45.130. Parameter-parameter asli pada pesan adalah dengan format <username><hostname><servername><realname>. *Username* diidentifikasi sebagai “sKuZ” dan *real name* sebagai “TeaM UniX b0at 0.4”.
7. Paket 12 yakni IRC server-irc.accesox.net (91.121.100.60) membalas ke *host* 192.168.45.130. Balasan berasal dari server “sex.accesox.net”, yang mengindikasikan pesan otorisasi oleh server.

Faktor Exacta *12 (2):* 145-155, 2019
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI : 10.30998/faktorexacta.v12i2.3549

8. Paket 15 yakni IRC server-irc.accesox.net melakukan ping terhadap *client* (192.168.45.130) dengan sebuah *hostname* karena server tidak dapat mengenali *hostname*. Perintah PING digunakan untuk menguji keberadaan *client bot*.
9. Paket 16 yakni respon PONG mengindikasikan sebuah balasan oleh *client bot* ke pesan PING dari server IRC.
10. Paket 18 merupakan komunikasi yang mengindikasikan balasan dari server "sex.accesox.net" yang tercipta pada "mar 25 2011 at 02:34:51 CET", yang mana server tersebut menjalankan "Unreal3.2.9-rc1" (sebuah server IRC open source). Server IRC menerima *client bot* dengan rentetan balasan. Seperti yang dinyatakan Christophe Kalt (2000) pada RFC 2812, rentetan balasan mengindikasikan keberhasilan registrasi dari client bot.
11. Paket 19 mengindikasikan bahwa pesan dari *client host* untuk mengubah *visibility mode* untuk pengguna tersembunyi pada server IRC.
12. Paket 21 dan 23 merupakan perintah JOIN yang dikeluarkan *client bot* dan permintaan untuk mulai mendengarkan kanal spesifik yakni "verga".
13. Paket 25 merupakan PRIVMSG yang digunakan oleh *client* untuk mengirim pesan pribadi ke kanal "verga". Pesan yang dikirimkan adalah dalam bahasa Spanyol yakni "NueVo PuTo InfeCcIoN".
14. Paket 27 berisi detail respon perintah dari server IRC. Mengindikasikan 56 *user* terlihat dan 189 *user* tak terlihat pada 9 server. Kemudian juga menginformasikan kepada *client host* bahwa *nickname* tidak terdaftar.
15. Paket 30 sampai 43 mengindikasikan registrasi ulang yang diinisiasi *client bot*
16. Paket 45 mengindikasikan pesan perintah dari *bot* "pLagUe" untuk mengunduh sebuah file *executable* yakni "plaga.exe" dari http://www.freewebtown.com/redzone/ ke dalam system drive dari client bot (C:\jiji).
17. Paket 53 berisi detail respon dari client bot ke server IRC yang menyatakan infeksi virus ke dalam "autorun.inf" dari USB *flash drive* yang terpasang.

HASIL DAN PEMBAHASAN

Ringkasan Komunikasi IRC

Ringkasan komunikasi IRC untuk paket-paket yang harus diperhatikan ditunjukkan pada gambar 2 dan gambar 3.

Faktor Exacta *12 (2):* 145-155, 2019
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI : 10.30998/faktorexacta.v12i2.3549

Packet nos.	Source	Destination	IRC command
6	192.168.45.130	91.121.100.60	PASS mierdaq
8	192.168.45.130	91.121.100.60	NICK pLagUe{USA}64007
10	192.168.45.130	91.121.100.60	USER SkuZ * ok .4.TeaM UniX b0at 0.4
12	91.121.100.60	192.168.45.130	:sex.accesox.net NOTICE AUTH :*** Looking up your hostname... :sex.accesox.net NOTICE AUTH :*** Checking ident... :sex.accesox.net NOTICE AUTH :*** No ident response; username prefixed with ~
15	91.121.100.60	192.168.45.130	:sex.accesox.net NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead PING :56EF9DAC
16	192.168.45.130	91.121.100.60	PONG 56EF9DAC
18	91.121.100.60	192.168.45.130	:sex.accesox.net 001 pLagUe{USA}64007 :Welcome to the AccesoX IRC Network pLagUe{USA}64007!~SkuZ@59.163.104.34
			:sex.accesox.net 002 pLagUe{USA}64007 :Your host is sex.accesox.net, running version Unreal3.2.9-rc1 :sex.accesox.net 003 pLagUe{USA}64007 :This server was created ven mar 25 2011 at 02:34:51 CET :sex.accesox.net 004 pLagUe{USA}64007 sex.accesox.net Unreal3.2.9-rc1 iowghraAsORTVSxNCWqBzvdHtGp lvhopsmntikrRcaqOALQbSeIKVfMCuzNTGjZ :sex.accesox.net 005 pLagUe{USA}64007 CMDS=KNOCK,MAP,DCCALLOW,USERIP UHNAMES NAMESX SAFELIST HCN MAXCHANNELS=16 CHANLIMIT=#:16 MAXLIST=b:60,e:60,I:60 NICKLEN=30 CHANNELLEN=32 TOPICLEN=307 KICKLEN=307 AWAYLEN=307 :are supported by this server :sex.accesox.net 005 pLagUe{USA}64007 MAXTARGETS=20 WALLCHOPS WATCH=128 WATCHOPTS=A SILENCE=15 MODES=12 CHANTYPES=# PREFIX=(qaohv)~&@%+ CHANMODES=beI,kfL,lj,psmntirRcOAQKVCuzNSMTGZ NETWORK=AccesoX CASEMAPPING=ascii EXTBAN=~,qjncrR ELIST=MNUCT :are supported by this server :sex.accesox.net 005 pLagUe{USA}64007 STATUSMSG=~&@%+ EXCEPTS INVEX :are supported by this server
19	192.168.45.130	91.121.100.60	MODE pLagUe{USA}64007 -ix
21	192.168.45.130	91.121.100.60	JOIN ##verga##
23	192.168.45.130	91.121.100.60	JOIN ##verga##
25	192.168.45.130	91.121.100.60	PRIVMSG ##verga## :.4.NueVo PuTo InfeCcIoN.

Gambar 2. Ringkasan Komunikasi IRC untuk Paket Hingga Nomor 25

Faktor Exacta *12 (2):* 145-155, 2019
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI : 10.30998/faktorexacta.v12i2.3549

27	91.121.100.60	192.168.45.130	:sex.accesox.net 251 pLagUe{USA}64007 :There are 56 users and 189 invisible on 9 servers :sex.accesox.net 252 pLagUe{USA}64007 8 :operator(s) online :sex.accesox.net 253 pLagUe{USA}64007 1 :unknown connection(s) :sex.accesox.net 254 pLagUe{USA}64007 30 :channels formed :sex.accesox.net 255 pLagUe{USA}64007 :I have 28 clients and 0 servers :sex.accesox.net 265 pLagUe{USA}64007 :Current Local Users: 28 Max: 196 :sex.accesox.net 266 pLagUe{USA}64007 :Current Global Users: 245 Max: 2976 :sex.accesox.net 372 pLagUe{USA}64007 :- This is the short MOTD. To view the complete MOTD type /motd :sex.accesox.net 372 pLagUe{USA}64007 :- :sex.accesox.net 376 pLagUe{USA}64007 :End of /MOTD command. :pLagUe{USA}64007 MODE pLagUe{USA}64007 :+ix :Global!services@accesox.net NOTICE pLagUe{USA}64007 :[.Random News. - Oct 14 2010] Registren sus nick de nuevo ... gracias. :NickServ!services@accesox.net NOTICE pLagUe{USA}64007 :Your nick isn't registered.
30	91.121.100.60	192.168.45.130	:pLagUe{USA}64007 MODE pLagUe{USA}64007 :-ix
33	192.168.45.130	91.121.100.60	MODE pLagUe{USA}64007 -ix
35	192.168.45.130	91.121.100.60	JOIN ##verga##
37	192.168.45.130	91.121.100.60	JOIN ##verga##
39	192.168.45.130	91.121.100.60	MODE pLagUe{USA}64007 -ix
41	192.168.45.130	91.121.100.60	JOIN ##verga##
43	192.168.45.130	91.121.100.60	JOIN ##verga##
45	91.121.100.60	192.168.45.130	:pLagUe{USA}64007!~SkuZ@59.163.104.34 JOIN :##verga## :sex.accesox.net 332 pLagUe{USA}64007 ##verga## :!downloaditz http://www.freewebtown.com/redzone/plaga.exe c:\jiji.exe 1 :sex.accesox.net 333 pLagUe{USA}64007 ##verga## ragebot 1298999449 :sex.accesox.net 353 pLagUe{USA}64007 @ ##verga## :pLagUe{USA}64007 :sex.accesox.net 366 pLagUe{USA}64007 ##verga## :End of /NAMES list. :sex.accesox.net 404 pLagUe{USA}64007 ##verga## :You need voice (+v) (##verga##)
48	192.168.45.130	91.121.100.60	MODE ##verga## -ix
50	91.121.100.60	192.168.45.130	:sex.accesox.net 482 pLagUe{USA}64007 ##verga## :You're not channel operator
53	192.168.45.130	91.121.100.60	PRIVMSG ##verga## :.4.{. USB.4 }.. Injected Virus into .4.autorun.inf.. on drive.4. D:
55	91.121.100.60	192.168.45.130	:sex.accesox.net 404 pLagUe{USA}64007 ##verga## :You need voice (+v) (##verga##)
58	91.121.100.60	192.168.45.130	PING :sex.accesox.net
59	192.168.45.130	91.121.100.60	PONG sex.accesox.net

Gambar 3. Ringkasan Komunikasi IRC untuk Paket Nomor 27

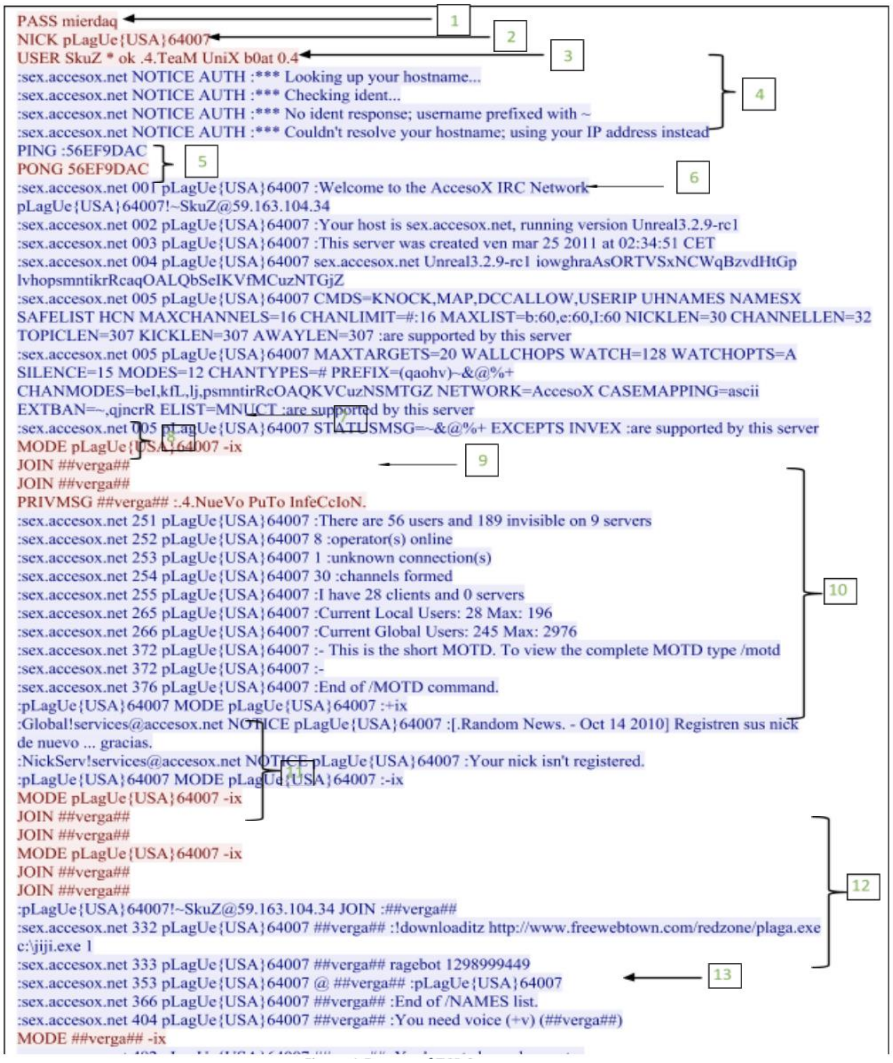
Interpretasi dari perintah-perintah IRC yang ditunjukkan pada gambar 2 dan 3 adalah seperti yang dinyatakan Christophe Kalt (2000) pada RFC 2812. Host pada 192.168.45.130 bergabung dengan irc.accesox.net (91.121.100.60) dengan *username* "sKuZ", kemudian masuk pada kanal "verga". *Bot* plague{USA}64007 menginstruksikan *client bot* (192.168.45.130) untuk mengunduh sebuah *executable file* "plaga.exe" dari http://www.freewebtown.com/redzone/, kemudian menyimpan *file* tersebut dalam *system drive* C:\jiji, dan menginjeksikan *file* tersebut ke dalam "autorun.inf" dari perangkat penyimpan yang terhubung melalui port USB (*flash drive*). Hal ini menunjukkan mekanisme propagasi *malware* dengan perantara *botnet. File* plaga.exe sendiri terdeteksi sebagai *malware* oleh COMODO Internet Security.

Berdasar observasi tersebut dapat disimpulkan bahwa *host* pada 192.168.45.130 melakukan sebuah *query* DNS ke 192.168.45.2 untuk resolusi dari irc.accesox.net. Dapat diasumsikan juga bahwa *host* pada 192.168.45.130 terinfeksi IRC Trojan yang melakukan inisiasi koneksi TCP ke irc.accesox.net, *logged* ke kancal IRC yang telah ditentukan, serta menyebarkan infeksi pada perangkat penyimpan yang terkoneksi melalui port USB, berdasar perintah dari *bot master*.

Faktor Exacta *12 (2):* 145-155, 2019
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI : 10.30998/faktorexacta.v12i2.3549

Analisis Sebuah *Excerpt* Aliran TCP

Sebuah *excerpt* dari aliran TCP ditunjukkan secara detail pada gambar 4, yang mengindikasikan 19 paket *client* dan 13 paket *server*.



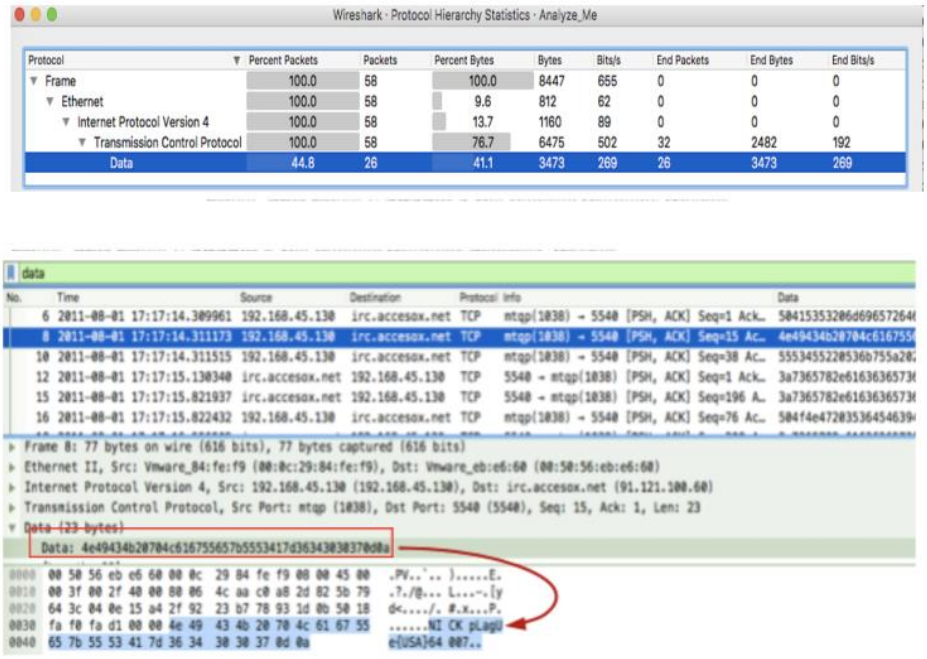
Gambar 4. *Excerpt* dari Aliran TCP

Keterangan:

1. *Password* koneksi yang ditentukan oleh *host bot*
2. *Nickname* yang ditentukan oleh *host bot*
3. *Username* yang ditentukan oleh *host bot*
4. Notifikasi oleh *server* IRC sex.accesox.net
5. Perintah PING dari server IRC dan balasan PONG dari *bot*
6. Informasi jaringan IRC
7. *Visibility mode* disembunyikan (ditentukan sebagai *hidden*) oleh *bot*
8. *Client* bot meminta pesan dalam rangka mulai memantau kanal spesifik yakni “verga”
9. Pesan pribadi dari *client bot* pada kanal “verga”
10. Pesan dari *botnet* pLagUe untuk mengunduh plaga.exe dari http://www.freewebtown.com/redzone/
11. Pesan pribadi dari client bot yang mengindikasikan keberhasilan injeksi dari plaga.exe kedalam autorun.inf dari empat buah perangkat yang tersambung melalui port USB

Faktor Exacta *12 (2):* 145-155, 2019
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI : 10.30998/faktorexacta.v12i2.3549

Pembacaan dari *excerpt* dari aliran TCP yang ditunjukkan pada gambar 4, pada dasarnya telah menunjukkan bahwa terjadi siklus botnet. Selanjutnya dilakukan analisis statistik terhadap hirarki protokol. Statistik hirarki protokol ditunjukkan pada gambar 5. Wireshark dapat menampilkan hirarki semua protokol yang dibaca sebagai pemeriksaan awal terhadap kegunaan masing-masing protokol pada jaringan yang dianalisis.



Gambar 5. Statistik Hirarki Protokol

Seperti ditunjukkan pada gambar 4, bahwa selain hirarki protokol juga ditunjukkan pembacaan data dari protokol yang ditampilkan. Pembacaan dari data protokol seperti ditunjukkan pada gambar 4 memastikan hasil pembacaan *excerpt* dari aliran TCP (gambar 3.), dimana berisi informasi keberadaan dan aktivitas *botnet*.

PENUTUP

Simpulan

Pada jaringan IRC publik dimana banyak terdapat serangan-serangan oleh *malware* maupun virus, perlu diketahui mekanisme pemicu serangan-serangan tersebut. Salah satu pemicu serangan-serangan tersebut adalah *botnet*. Berdasarkan pengamatan dan analisis terhadap jaringan IRC dengan alat bantu Wireshark maka dapat ditampilkan *excerpt* dari aliran TCP, serta data dari semua protokol tertangkap, yang tersusun secara hirarkis. Berdasar pemahaman terhadap pembacaan Wireshark dengan disesuaikan terhadap RFC 2812, dapat diketahui informasi mengenai aktivitas *botnet* pada lalu lintas jaringan IRC. Dengan diketahuinya aktivitas *botnet* pada jaringan IRC, maka selanjutnya dapat digunakan sebagai acuan pembuatan aturan-aturan pada pengelolaan jaringan, seperti misalnya aturan-aturan pada *firewall*, aturan-aturan pada mekanisme *routing*, aturan-aturan pada pengelolaan *server*, dan sebagainya.

DAFTAR PUSTAKA

Alothman, Basil & Rattadilok, Prapa. (2017). Towards using Transfer Learning for Botnet Detectoin. *12th International Conference for Internet Technology and Secured Transaction* (ICITST-2017). University of Cambridge, Cambridge

Puri, Ramneek. (2003). *Bots &; Botnet: An Overview.* SANS Institute, Singapore

Kasperzyk, Rafal., Paz, Marcin., dan Tarapata, Zbigniew. (2017). Modelling and simulation of botnet based cyber-threats. *MATEC Web Conferences Volume 125*, *21st International Conference on Circuits, Systems, Communications and Computers (CSCC 2017)*. Crete: e∞ sciences

Kamluk, Vitaly. (2008, 18 Juli). Biznes botnetnowy. [online] Tersedia di https://tech.money.pl/hi-tech/artykul/biznes-botnetowy,212,0,356308.html [Diakses 27 Juni 2019]

Sfakianakis, Andreas., Douligeris, Christos., Marinos, Louis., Lourenço, Marco., & Raghimi, Omid. (2019). *ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends.* DOI: 10.2824/622757

Godkin T., (2013), *Statistical Assessment of Peer-to-Peer Botnet Features*, University of Victoria

Bloice, Graham., 2019. Tshark Command Line using PowerShell, [online] Tersedia di: <https://sharkfesteurope.wireshark.org/assets/presentations17eu/33.7zl> [Diakses 18 Februari 2019]

Kalt, C. 2000. RFC 2812-Internet Relay Chat: Client Protocol – IETF Tools, [online] Tersedia di: https://tool.ietf.org/html/rfc2812 [Diakses 21 Januari 2019]