Pengesanan Botnet P2P Menggunakan Teknik Pengenalpastian Nilai Ambang

Wan Ahmad Ramzi Wan Yusuf
Kolej Komuniti Masjid Tanah
ramzi016@gmail.com

Mohammad Hairy Kharauddin
Kolej Komuniti Masjid Tanah
airis1482@yahoo.com

Mohd Rizal Dolah
Kolej Komuniti Masjid Tanah
rizal@kkmt.edu.my

Abstract
P2P Botnet or 'Peer to Peer' Botnet is known as one of the most dangerous threats to computer network technology. Previously, several detection techniques have been proposed to detect its presence. One of the techniques focused is on feature sets as a detection mechanism. However, previous studies highlighted feature detection for this Botnet family found that there is a lack of research on the threshold value feature as botnet detection. Research so far tends to focus on detection features rather than analysis on the feature itself. In this study, identifying threshold values for P2P Botnet detection is based on seven bot samples and 52 features taken from the observed network traffic. suggests methodologies consisting of feature selection modules, logistics regression modules and threshold value identification. The approach successfully identifies a set of features to detect P2P Botnets. The traffic observation test shows that P2P Botnet detection is based on the pushed_data_pkts_b2a and pure_act_pkts_a2b features where the threshold cutting value for both is at 80% detection rate which contributes to the detection of botnet P2P botnet detection at a higher rate.

Keywords: P2P botnet, threshold value, feature selection

Abstrak
P2P Botnet ataupun 'Peer to Peer' Botnet dikenali sebagai salah satu ancaman jahat terhadap teknologi rangkaian komputer. Sebelum ini, beberapa teknik pengesanan telah dicadangkan untuk mengesan kehadirannya. Salah satu teknik difokuskan adalah pada set fitur sebagai mekanisme pengesanan. Namun, kajian sebelumnya menyoroti pengesanan fitur bagi family Botnet ini mendapati terdapat kekurangan kajian berkenaan ciri nilai ambang sebagai pengesanan botnet. Penyelidikan setakat ini cenderung memusatkan perhatian pada ciri pengesanan daripada analisis pada ciri itu sendiri. Dalam kajian ini, mengenal pasti nilai ambang untuk pengesananP2P Botnet adalah berdasarkan tujuh sampel bot dan 52 ciri diambil dari trafik rangkaian yang dicerap. mencadangkan metodologi pengesanan terdiri daripada modul pemilihan ciri, modul regresi logistik dan pengenalan nilai ambang. Pendekatan berjaya mengenal pasti set ciri untuk mengesan Botnet P2P. Ujian pencerapan trafik menunjukkan pengesanan Botnet P2P adalah berdasarkan fitur *pushed_data_pkts_b2a* dan *pure_act_pkts_a2b* yang mana nilai pemotongan ambang bagi

kedua dua adalah pada kadar pengesanan 80% iaitu menyumbang kepada pengesanan Botnet P2P botnet pada kadar yang lebih tinggi.

Katakunci: botnet P2P, nilai ambang, pengesanan fitur

1.0 Pengenalan

Komputasi Peer-to-peer (P2P) muncul dengan banyak penggunaan dan botnet memanfaatkan teknologi ini dengan memperkenalkan botnet P2P yang terdiri dari rangkaian P2P yang akan digunakan untuk mengendalikan bot kemudian menjadi ancaman terhadap jaringan komputer. Kebiasannya, Botnet P2P biasanya terlibat dengan kegiatan jenayah seperti serangan DDoS, penipuan klik, penyebaran spam dan juga mencuri maklumat peribadi pengguna. (Saad et al. 2011) Jika dibandingkan dengan botnet tradisional dan botani yang lain, ianya lebih sukar dikesan.

Umumnya, Botnet jenis ini adalah daripada seni bina terpusat yang terdiri daripada titik kegagalan pusat. Ini akan menjadikan pelayan C&C lebih mudah untuk mengesan semua jenis botnet. Walau bagaimanapun, botnet berusaha menghindari seni bina terpusat dengan meniru seni bina P2P dan mekanisme kawalan. Ini kerana tidak ada node terpusat untuk arahan dan kawalan dalam seni bina rangkaian P2P dengan setiap bot peer bertindak sebagai klien dan pelayan (Elhalabi, Manickam, Melhim, Anbar & Alhalabi, 2017).

Dengan melakukan itu, bot dapat dimanipulasi oleh 'Botmaster' ataupun pengawal komputer untuk menyebarkan perintah kepada rakan jaringan seterusnya dan dapat mengumpulkan maklumat yang berguna dan menjadikan botnet P2P menawarkan ketahanan yang lebih tinggi walaupun sebahagian 'Bot' terganggu, masih ada lebih banyak 'Bot' yang dapat saling menghubungi dan berkomunikasi dengan 'Botmaster' (J. Zhang et al. 2014).

Sebuah syarikat keselamatan siber telah melaporkan pada suku kedua 2017 bahawa organisasi melaksanakan aplikasi P2P yang terdedah kepada malware dan ancaman family botnet adalah tujuh kali lebih banyak daripada organisasi yang tidak menggunakan aplikasi P2P (Fortinet, 2017). Selanjutnya, pengesanan botnet P2P menjadi lebih mencabar kerana 'Botmaster' menyebarkan enkripsi untuk komunikasi mereka antara bot (Vaziri,2017). Ancaman botnet P2P akan terus berkembang untuk menghindari pengesanan dan memberikan kerumitan dalam setiap serangan yang dilakukan.

Salah satu tekniknya adalah dengan memilih ciri pengesanan sama ada dalam log proses host atau log rangkaian (R. S. Abdullah et al. 2013 & (Karim et al. 2014). Walau bagaimanapun, terdapat kekurangan dalam analisis ambang untuk setiap ciri yang dipilih itu sendiri. Kepentingan nilai ambang boleh menyumbang untuk mencari ciri sebenar pengesanan botnet. Penyelidikan dilakukan untuk mencari kaedah yang lebih cekap bertujuan mengenali kehadiran botnet dalam komunikasi rangkaian. Kajian ini adalah untuk membezakan tingkah laku Botnet P2P dalam trafik rangkaian melalui pengenalpastian ambang ciri.

2.0 Kajian Literasi

P2P Botnet adalah kumpulan bot yang berkomunikasi berdasarkan seni bina terdesentralisasi menggunakan protokol peer-to-peer. Pengesanan optimum ambang berdasarkan pengesanan anomali untuk menentukan ambang dalam melaksanakan sistem dinamik dalam menghadapi serangan strategik. Metodologi dirumuskan sebagai pembela penyerang untuk menentukan ambang dengan mencapai pertukaran optimum antara penundaan pengesanan dan kadar positif palsu. Untuk mengoptimumkan nilai ambang, penggunaan algoritma yang mengira ambang tetap optimum tidak bergantung pada masa yang asilnya menunjukkan bahawa pendekatan ambang batas adaptif mendapatkan penangguhan pengesanan keseluruhan yang lebih baik-pertukaran positif palsu dan meminimumkan kerugian.

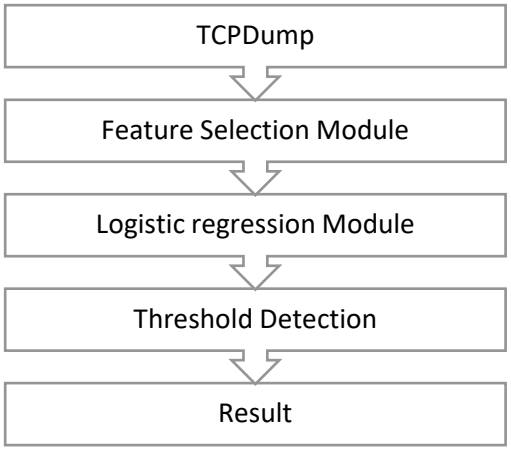
Sementara itu cadangkan teknik baru dalam mengenal pasti nilai ambang statik dari ciri yang diturunkan dalam serangan pantas pada perspektif korban. Teknik baru ini menunjukkan nilai ambang terpilih yang tepat pada fitur pengaruh memberikan sumbangan untuk pengesanan 'Intrusion Detection System' untuk mengesan anomali dalam rangkaian. Pendekatan ini terbukti dalam mengenal pasti serangan pantas dalam masa nyata.

(Staniford, Hoagland & McAlerney, 2002) mencadangkan pengesanan Anomali statistik Anomali Rangkaian yang menggunakan teknik anomaly bagi mengira skor untuk setiap paket yang melintasi trafik dan dimajukan untuk tujuan pengesanan ancaman apabila nilai ambang melintasi hadnya.

Menurut (Wang, 2005), kajian ini menggunakan pendekatan pemodelan regresi logistik Multinomial untuk pengesanan pencerobohan anomali. Objektif utama adalah untuk menentukan potensi faktor risiko yang berafiliasi secara signifikan dengan serangan dan serangan prestasi dalam klasifikasi serangan. Jenis data yang digunakan untuk carian semula ini adalah pemboleh ubah bersandar dari pemboleh ubah kategori tidak tersusun berdasarkan data 1999 KDD-cup. Model yang dicadangkan mengira skor risiko untuk profil tingkah laku pengguna dan menghasilkan pengesanan pencerobohan yang lebih baik dan meningkatkan keselamatan bagi pengguna.

3.0 Metodologi

Di bahagian ini, pendekatan kajian adalah untuk mengenal pasti nilai ambang untuk pengesanan P2P Botnet. Rajah 1 menunjukkan keseluruhan metodologi yang digunakan dalam kajian ini.



Rajah 1: Metodologi mengenal pasti ambang

Pengesanan Botnet P2P disesuaikan berdasarkan metodologi yang dicadangkan oleh (M. A. et al.2010). Kajian sebelumnya terdiri daripada lima modul utama dengan tujuan untuk mengesan aktiviti pencerobohan serangan pantas dan disasarkan pada Modul Berasaskan Masa dan modul pengesanan Ambang. Modul yang diadaptasi dari pengkaji sebelumnya adalah modul TCPDUMP, Modul Pengekstrakan Ciri dan modul Ambang. Walau bagaimanapun, modul berdasarkan masa telah digantikan oleh modul regresi Logistik agar sesuai dengan kajian ini. Pemilihan 'Feature' yang menerapkan teknik perlombongan data dan fungsi modul regresi Logistik adalah dengan cara yang paling sesuai untuk menentukan ciri-ciri yang signifikan sementara modul Deteksi Ambang adalah untuk membezakan antara lalu lintas normal dan tidak normal dalam serangan botnet P2P. Modul Hasil mengandungi hasil pengesanan.

3.1 Tcpdump

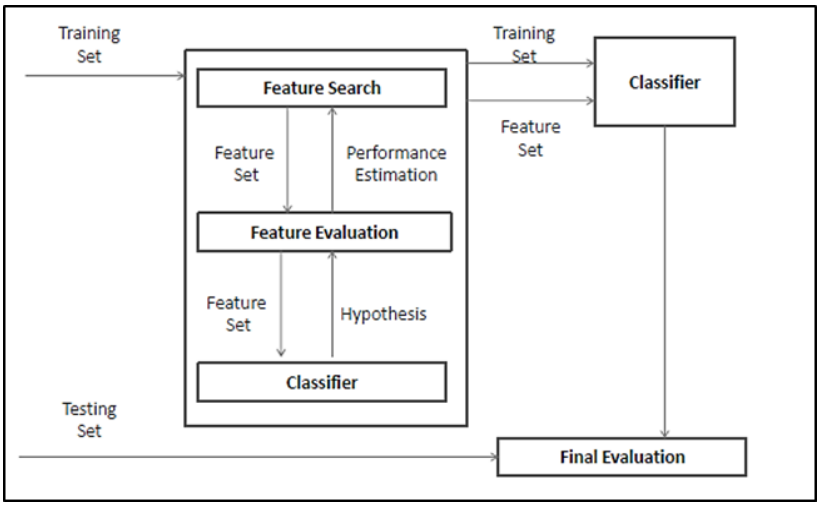
Tcpdump adalah alat mengendus paket yang digunakan oleh pentadbir rangkaian untuk mengendus dan menganalisis lalu lintas di rangkaian (C.Gandhi,2014)&(A.Lazzez,2013) memungkinkan untuk melihat apa yang berlaku di rangkaian dan benar-benar berguna untuk menyelesaikan banyak jenis masalah termasuk masalah yang bukan disebabkan oleh komunikasi rangkaian. Aplikasi 'Tcpdump' dapat membaca dan menulis trafik rangkaian masa nyata menggunakan perpustakaan libpcap yang mampu menangkap lalu lintas rangkaian dalam masa nyata dan disimpan ke fail (M.A.et al.2010). Libpcap pada awalnya dikembangkan oleh pembangun 'tcpdump' dalam kumpulan rangkaian pengkajian di 'Lawrence Berkeley Laboratory'. Tangkapan paket tingkat rendah, pembacaan tangkapan fail, dan penulisan kod penulisan fail tcpdump diekstrak dan dibuat menjadi perpustakaan, dengan mana tcpdump dihubungkan dan dikembangkan oleh kumpulan ini iaitu pengkaji yang sama yang mengembangkan 'tcpdump'. Dalam kajian ini, modul tcpdump berfungsi membaca dan mentafsirkan trafik rangkaian

mentah dari bentuk binari ke ASCII untuk membolehkan kandungan maklumat lalu lintas dapat difahami. Fail ini ditukar menjadi log parser (.csv) menggunakan alat tcptrace sebelum menjalani modul pemilihan ciri. Gambaran setiap botnet seperti yang dinyatakan dalam Jadual 1.

3.2 Feature Selection Module

Fungsi fungsi modul pemilihan mampu menghilangkan ciri-ciri berlebihan dan tidak perlu yang juga menggambarkan sebagai proses memilih subkumpulan ciri yang berkaitan yang menyumbang dalam elemen NIDS dan mempunyai data palsu dan data berlebihan. Ini boleh mengakibatkan korelasi palsu yang akan mengganggu proses pembelajaran pengklasifikasi

Modul Pemilihan Ciri ini, model Wrapper dipilih kerana mengoptimumkan pengklasifikasi dan mampu menangani data dimensi besar. Kami menerapkan teknik pemilihan ke depan yang bermula dari set fitur kosong kemudian secara beransur-ansur meningkatkan set fitur. Enam ciri dipilih setelah menjalani proses ini yang mana ciri yang paling dipilih sebagai hasil akhir modul. Prestasi penilaian yang lebih baik untuk proses pemilihan ciri menghasilkan ketepatan keseluruhan pada 98.75% yang merupakan kadar pengesanan serangan yang sangat tinggi. Rajah 2 menggambarkan kerangka umum untuk kaedah pembungkus yang disesuaikan dari (Kohavi & John,1997). Pendekatan ini memerlukan pencarian ciri yang dipilih daripada 52 ciri rangkaian. Tiga komponen terlibat mengikut gambar tersebut iaitu pencarian ciri, penilaian ciri, dan klasifikasi.



Rajah 2: Kerangka umum untuk kaedah pembungkus

3.3 Modul Logistic Regression

Fungsi Modul regresi logistik adalah untuk menganalisis set data yang mempunyai satu atau lebih parameter bebas untuk menentukan hasil

dikotom di mana hanya ada dua kemungkinan nilai 1 (BENAR, Serangan) atau 0 (SALAH, normal). Ini juga merupakan teknik untuk mencari sistem probabilistik model yang paling sesuai untuk meramalkan peristiwa masa depan. Modul ini menggunakan regresi logistik binari untuk menyaring semua ciri yang dipilih dalam modul pemilihan ciri dan cuba mencari ciri signifikan terbaik dengan pengesanan ketepatan terbaik. Ciri-ciri penting yang dipilih kemudian akan digunakan dalam Modul Pengesanan Ambang. Ujian kebaikan dan jadual klasifikasi telah digunakan untuk mengesahkan pemilihan ambang untuk kategori ini.

3.4 Modul threshold detection

Modul ini diklasifikasikan sebagai ambang Klasifikasi yang mana data dari model regresi logistik telah dipasang dan dikelompokkan menjadi dua kelas 'normal' dan 'serangan' menggunakan kemungkinan kejadian yang ditentukan atau dianggarkan. Persamaan regresi model berdasarkan persamaan:

$$P = (Y) = (e \wedge (\beta\_1 + \beta\_0 X)) / (1 + e \wedge (\beta\_1 + \beta\_0 X))$$

Di mana:

P (Y) menunjukkan kebarangkalian kejayaan serangan.
β_0 ialah pemalar persamaan.
β_1 menunjukkan kecerunan fungsi logistik

Bentuk alternatif dari persamaan regresi logistik diberikan oleh Ramsey dan shafer, (2002)

$$Logit (Y) = (\beta\_0 + \beta\_1 X\_1 + Ei)$$

Di mana:

β_0 ialah pemalar persamaan
β_1 adalah coeficcient dari pemboleh ubah peramal
X_1 adalah pemboleh ubah ramalan

Data ini paling kerap dianggarkan untuk data binari, dan juga dikenali sebagai ambang kejadian.(Toms & Villard, 2018) Meletakkan nilai ambang yang rendah boleh menghasilkan positif positif yang berlebihan sementara meletakkan terlalu tinggi, ini boleh menyebabkan sistem kehilangan pengimbas yang kurang agresif (Jung, PaxsonBerger & Balakrishnan,2004). Oleh yang demikian, adalah penting memilih nilai ambang yang sesuai untuk mengesan aktiviti serangan botnet P2P.

Model yang dipasang dari modul regresi logistik digunakan untuk melukis graf kebarangkalian menggunakan persamaan regresi logistik untuk mengenal pasti lalu lintas yang tidak normal.

4.0 Hasil dan perbincangan

Hasil untuk model pengesanan dinilai oleh metrik pengukuran prestasi seperti jadual klasifikasi. Ketepatan pengesanan yang lebih tinggi bermaksud bahawa model itu baik untuk meramalkan tingkah laku tidak normal dalam lalu lintas rangkaian dan dapat mengesan serangan botnet P2P secara berkesan.

Dalam eksperimen ini, lalu lintas rangkaian normal dan bot diproses dan terdapat tujuh varian Botnet P2P yang telah dikenal pasti untuk digunakan dalam eksperimen ini. Gambaran setiap botnet seperti yang dinyatakan dalam Jadual1. Sementara itu, lalu lintas P2P normal dihasilkan dengan menjalankan aplikasi P2P standard pada host komputer dengan antivirus yang diaktifkan. Ini untuk memastikan tidak ada aktiviti jahat dalam lalu lintas yang ditangkap. Lalu lintas jaringan dilabel sebagai "0" untuk P2P normal dan 1 untuk bot P2P.

Jadual 1: Botnet yang digunakan dalam kajian ini

Botnet Variance	Description
Crypto Wall	Crypto Wall is a Trojan horse that able to encrypt files in the affected computer and later will ask users to pay for decrypt the files. This botnets mostly infect by exploiting kits hosted through malicious code, spam mails and other malware. (F. I. Editors,2015)
Kelihos	Kelihos botnet are also called as Hlux, this botnet included in the steal of bitcoins and spamming. Kelihos botnet is a P2P botnet which mean the individual nodes in botnet able to act as a C&C server to the botnet. At first this botnet was mainly involved in email spam and DDOS attack but later, the botnet was upgraded and this botnet able to perform stealing bitcoins wallet as well as a program used to mine bitcoins itself.
Neris	Neris used an HTTP based C&C channel and not an IRC C&C channel. The activities of the botnet were to communicate using several C&C channels and then to try send it to SPAM which eventually send SPAM and performing click-fraud using some advertisement services. (P. Aswal and A. Bijalwan,2016)
Rbot	Rbot is a group of backdoor Trojan that focuses on version of Microsoft Windows. After Rbot infected the computer, the computer will become controllable to attacker through an IRC channel. Usually order will be given by botmaster to spread to

	others computers by examining for network share with weak password and also abusing different vulnerabilities. Attackers will also perform other action such as DDOS. (M. Senthilkumar et al. 2015)
Tbot	Tbot is also a Trojan horse that opens a secondary passage on the infected PC to download and install extra malware and filch data. This botnet also associate with an IRC and get commands by performing activities such as download and execute files from a remote location, download and inject files into running process, connect to an arbitrary URL and take data from the infected computers and send it to the remote attacker.
Zbot	Zbot also known as Zeus, this botnet runs on Microsoft Window version and a family of Trojans that created by tool kits knowns as "Zeus". Zbot used different method to infect computers. It infest computer via spam, drive-by download and downloaded another malware. Mostly attackers behind Zbot usually will spread their threat through spam campaign. Drive-by downloads is occurred when user visit of the infected website. It mostly used to steal classified information from the infected computers especially online certificates, banking information and system information but it also able to steal other data that the attackers needs. (Trend Micro Inc,2009)&(S. Nagendra Prabhu and D. Shanthi,2015)
ZeroAccess	ZeroAccess is a botnet that affects Microsoft Windows operating system. It uses an advanced rootkit to hide itself in infected computers. ZeroAccess spread via web that had been infected and redirect traffic to a malicious web then in turn distribute it using toolkit called Black hole Exploit Toolkit and the Bleeding Life Toolkit. ZeroAccess also up-date itself using P2P network which allow the attackers to continually using ZeroAccess to perform any illegal activities. There are two main operation of ZeroAccess which is Bitcoin mining and Click fraud. Computers that have been infected will generate Bitcoins for the botnet controller and used click fraud to stimulate clicks on advertisement website that paid for per click basic. (P. Pearce,2014)&(A. Neville and R. Gibb,2013)

Dalam modul pemilihan ciri, kami memperoleh enam fitur seperti yang ditunjukkan dalam Jadual 2. Perhatikan bahawa a2b adalah paket yang mengalir dari host a ke host b sementara b2a adalah paket yang mengalir dari host b ke host a .

Jadual 2: Ciri terpilih dalam modul pemilihan ciri.

Feature name	Description
pushed_data_pkts_a2b	The count of all the packets seen with the PUSH bit set in the TCP header.
pushed_data_pkts_b2a	The count of all the packets seen with the PUSH bit set in the TCP header.
Max_Win_Adv_a2b	The largest window advertisement that was sent from the destination to the source
Max_Win_Adv_b2a	The largest window advertisement that was sent from the destination to the source
pure_act_pkts_a2b	The total number of ACK packets sent between the hosts that were not piggy-backed with data (just the TCP header and no TCP data payload) and did not have any of the SYN/FIN/RST set.
throughput_b2a	The average throughput calculated as the unique bytes sent divided by the elapsed time i.e., the value reported in the unique bytes sent field divided by the elapsed time (the time difference between the capture of the first and last packets in the direction).

Dalam modul regresi logistik, Pengaruh ciri yang paling signifikan untuk mengesan botnet P2P dalam rangkaian akan ditemui. Apabila kualiti regresi logistik bertambah baik, hanya ciri penting yang dimasukkan dalam persamaan regresi logistik. Dalam kajian ini, ciri-ciri Pushed_data_pkts_a2b, push_data_pkts_b2a dan pure_act_pkts_a2b sementara tiga ciri lain max_win_adv_a2b, max_win_adv_b2a dan throughput_b2a dianggap tidak menambah ketara pada model.

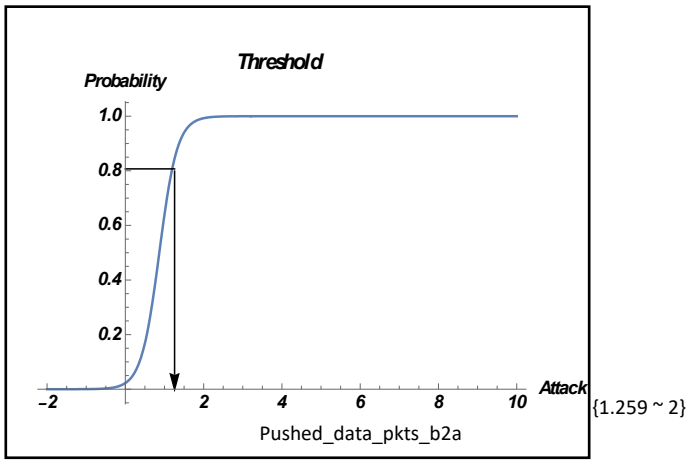
4.1 Identifikasi threshold bagi fitur pushed_data_pkts_b2a

Rajah 3, menunjukkan ciri pengaruh kedua, Pushed_data_pkts_b2a yang dihasilkan oleh persamaan regresi logistik yang sesuai untuk mengenal pasti ambang batas sebagai garis dasar untuk membezakan lalu lintas normal dan tidak normal dalam rangkaian. Persamaan regresi logistik yang mengira ambang adalah:

$$P(Y) = e \text{ ^ } (-3.763 + 4.339x) \;/\; (1 + e \text{ ^ } (-3.763 + 4.339x))$$

$$\text{Logit } (Y) = (3.763 + 4.339X1)$$

Ambang batas untuk ciri ini dikenal pasti apabila kebarangkalian 80% diterapkan pada model.



Rajah 3: Threshold bagi fitur Pushed_data_pkts_b2a

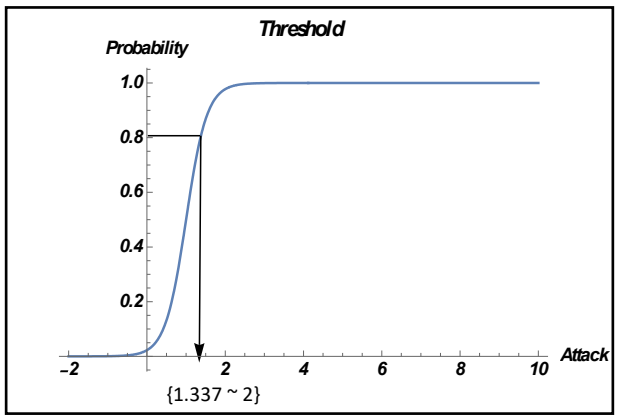
Nilai pemotongan adalah 1.259 dan oleh itu pemilihan 2 paket sesaat yang dibuat oleh tuan rumah tunggal dapat dianggap sebagai serangan, sementara jika nilai jatuh di bawah nilai ambang dianggap normal.

4.2 Identifikasi threshold pure_act_pkts_a2b

Rajah 4 menunjukkan grafik yang dihasilkan dari regresi logistik yang dipasang untuk ciri pure_act_pkts_a2b. Persamaan logistik yang menghasilkan graf adalah:

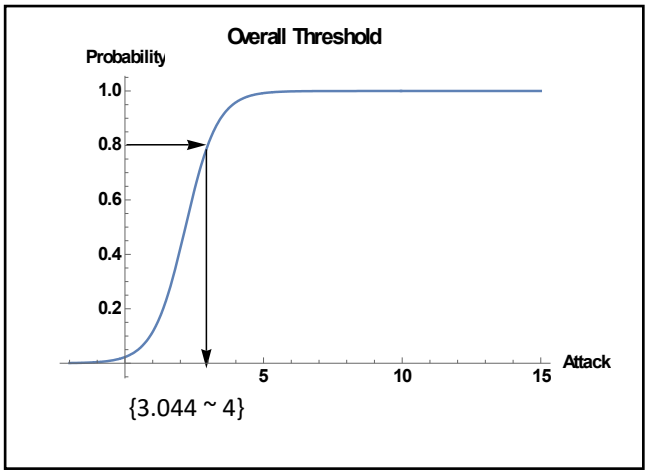
$$P(Y) = e^{(-3.763 + 3.763x)} / (1 + e^{(-3.763 + 3.763x)})$$

$$\text{Logit}(Y) = (3.763 + 3.763X1)$$



12

Rajah 4: Threshold bagi fitur (pure_act_pkts_a2b)



Rajah 5: Threshold keseluruhan bagi fitur (Pushed_data_pkts_b2a, pure_act_pkts_a2b)

Kesimpulan

Kesimpulannya, kajian ini mendedahkan beberapa ciri yang dipengaruhi untuk P2P Botnet Detection. Didapati bahawa model model fitting menghasilkan yang paling sesuai untuk data. Ujian lalu lintas sebenar yang membuktikan bahawa pengesanan botnet P2P ditentukan oleh pushed_data_pkts_b2a dan pure_act_pkts_a2b dengan kedua-duanya pada nilai pemotongan ambang pada kadar pengesanan 80%. Untuk menyimpulkan bahawa, hasil analisis menunjukkan ciri yang dihasilkan memberikan sumbangan yang baik dalam pengesanan botnet P2P dengan kadar pengesanan yang lebih tinggi, sehingga memenuhi tujuan penyelidikan. Penilaian yang baik terhadap kadar pengesanan tidak berarti dapat digunakan dalam pengesanan kerana akan menghasilkan pengesanan penggera yang salah. Ia masih memerlukan peningkatan dalam mengembangkan teknik yang lebih baik untuk mengenal pasti nilai ambang yang dapat mengesan pelbagai jenis Botnet sambil meningkatkan kadar pengesanan. Oleh kerana kajian ini hanya memfokuskan pada protokol TCP, tujuannya adalah menerapkan protokol lain seperti UDP. Selain itu, dalam penyelidikan masa depan, kami bertujuan untuk melihat log IDS, untuk menentukan ambang yang sesuai dalam lalu lintas yang dapat menyumbang kepada ketepatan pengesanan IDS untuk membezakan aktiviti normal dan tidak normal dalam rangkaian.

Rujukan

Saad, S., Traore, I., Ghorbani, A., Sayed, B., Zhao, D., Lu, W., Felix, J. & Hakimian, P. (2011). Detecting P2P botnets through network behavior analysis and machine learning, *In 2011 9th Annual International Conference on Privacy, Security and Trust* (pp.174–180). Fredericton, Canada.

Elhalabi, M. J., Manickam, S., Melhim, L. B., Anbar, M. & Alhalabi,V (2013) A review of peer-to-peer botnet detection techniques, *Journal of Computer Science,10*(1), 169–177.

Zhang, J., Perdisci, R., Lee, W., Luo, X. & Sarfraz, U. , (2014). Building a scalable system for stealthy P2P-botnet detection, *IEEE Trans. Inf. Forensics Secur., 9*(1), 27–38.

Vaziri, S.,(2017). *Botnets.Retrive from* https://labs.ripe.net/Members/alireza_vaziri/botnet.

Abdullah, R. S., Abdollah, M. F., Noh, Z. A. M., Mas'ud, M. Z., Sahib, S., & Yusof, R. (2013) Preliminary study of host and network-based analysis on P2P botnet detection. *In International Conference. Technology Informatics, Management Engineering Environment* (pp. 105–109). Bandung, Indonesia

Suarez-Tangil, G., Palomar, E., Ribagorda, A. &. Sanz, I. (2015) Providing SIEM systems with self-adaptation. *Inf. Fusion, 21* (pp. 145–158)

Karim, A., Salleh, R., Shiraz, M., Shah, S. A. A., Awan, I., & Anuar, N. B. (2014). Botnet detection techniques: review, future trends and issues. *Journal Zhejiang Univ. Sci. C, 15*(11), 943–983

Staniford, S., Hoagland, J. A. & McAlerney, J. M.(2002). Practical automated detection of stealthy portscans, *Journal Computer. Security,10* (1-2), 105–136.

Wang, Y. (2005). A multinomial logistic regression modeling approach for anomaly intrusion detection, *Computer Security, 24*(8), 662– 674.

Gandhi, C., Suri, G., Golyan, R. P., Saxena, P., & Saxena, B. K. (2014) Packet sniffer – a comparative study, *International Journal Computer Networks Communication. Security, 2*(5)179–187

Lazzez, A. (2013) A survey about network forensics tools, *International Journal Computing Information Technology, 2*(1)2279–764.

Kohavi, R., & John, G. H., (1997) Wrappers for feature subset selection *Artif. Intell., 97*(1–2), 273–324, 1997.

Ramsey, F & Schafer, D. (2012) *The statistical sleuth: a course in methods of data analysis*. Cengage Learning,

Toms, J. D., & Villard, M.(2015) Threshold Detection: Matching Statistical Methodology to Ecological Questions and Conservation Planning Objectives, *Avian Conserv. Ecol., 10*(1), 1–8.

Jung, J. J., Paxson, V., Berger, A. W., & Balakrishnan, H. (2004) Fast portscan detection using sequential hypothesis testing, *IEEE Symp. Secur. Privacy,* (pp. 1–15). Berkeley, California.

Editors, F. I. (2015) CryptoWall crimeware netted US$325M in revenue: report, *Fintech Innovation*, 2015. Retrive from http://www.enterpriseinnovation.net/article/cryptowall-crimeware-netted-us325m-revenue-report-378336026.

Aswal, P. & Bijalwan, A.,(2016) Bitcoin mining based botnet analysis, *Int. Journal Comput. Appl.,145*(6), 23–27.

Senthilkumar, M., Ramasamy, V., Sheen, S., Veeramani, C., Bonato, A. & Batten, L. (2015). Computational intelligence, cyber security and computational models: *In Advances in Intelligent Systems and Computing, 2016, vol. 412.*

Trend Micro Inc, Web Threat Spotlight - ZBOT/Zeus Sends Out Tailor-Made Spam,2009.

Nagendra, S., Prabhu & Shanthi, D.(2015). Examining zeus botnet by adopting key extraction and malicious traffic detection framework using DNS, *Int. J. Appl. Eng. Res.*, *10*(3), 6987–7007.