Menangani Ancaman Conficker Terhadap Organisasi Menggunakan Sistem Pengesanan Dan Pencegahan Pencerobohan Berasaskan Rangkaian Snort

Hafezudeen bin Usak
Rossilawati Sulaiman

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Penyediaan dan penggunaan perkhidmatan berasaskan atas talian oleh sesebuah organisasi sama ada jabatan kerajaan mahupun pihak swasta telah menunjukkan peningkatan yang amat ketara. Seiring dengan itu, ancaman keselamatan terhadap infrastrukur teknologi maklumat organisasi telah menunjukkan peningkatan yang ketara pada setiap tahun. Secara tidak langsung ianya memerlukan setiap organisasi memelihara tahap ketersediaan serta keselamatan aset teknologi maklumatnya supaya sentiasa berada berada dalam keadaan terbaik dan selamat. Antara ancaman keselamatan yang sering dihadapi oleh sesebuah organisasi terhadap aset maklumat mereka adalah perisian hasad yang mana ianya termasuklah virus, *trojan horse*, *worm* (Cecacing), *rootkit*, *scareware* dan *spyware*. Jenis perisian hasad yang menunjukkan peningkatan ketara adalah cecacing Conficker yang mana Malaysia merupakan negara penyumbang kedua tertinggi di bawah UAE. Sehubungan dengan itu, kajian ini dijalankan bertujuan untuk menganalisa dan mengkaji aktiviti rangkaian dan gerak kerja komputer yang telah dijangkiti oleh cecacing Conficker serta menghasilkan set petua sistem pengesanan dan pencegahan pencerobohan berasaskan rangkaian menggunakan Sistem Snort untuk menangani ancamannya. Bagi memenuhi objektifnya, sampel cecacing serta data trafik yang dijana oleh komputer yang dijangkiti telah dianalisis dan dikaji seterusnya melaksanakan proses penghasilan dan pengujian terhadap set petua yang dihasilkan dalam kajian ini bagi menangani ancaman Conficker. Kajian ini juga mendapati cecacing ini bergantung sepenuhnya terhadap komputer yang dijangkiti untuk memulakan sebarang proses komunikasi dalam menerima sebarang binari dan muat beban. Oleh yang demikian, penghasilan set petua dalam kajian ini menumpukan untuk menghalang trafik hasad yang dihantar oleh komputer yang dijangkiti untuk memulakan proses komunikasi tersebut.

Kata kunci: perisian hasad, Conficker, analisa perisian hasad, sistem pengesanan dan pencegahan pencerobohan berasaskan rangkaian

ABSTRACT

Provision and use of on-line based services either by government departments or the private sector has shown significant impovement. Along with that, security threat to the organization's information technology infrastructure has shown a significant increase each year. Indirectly, it would require each organization to maintain a level of availability and security of its information technology assets to always be in the best condition and safe. Among the security threats faced by an organization for their information assets is malware which includes viruses, trojan horses, worms, rootkit, spyware and scareware. One of the malware's type which shows a significant increase lately is Conficker's worm, where Malaysia is the second highest contributor's countries under UAE. Therefore, this study aimed to analyze and review the network activity and workflow of computers that have been infected by the Conficker worm then produces a set of rules for network-based intrusion detection and prevention system (Snort) to address the threat. To meet its objectives, the worm samples and traffic generated by infected computers have been analyzed and reviewed followed by the production and testing processes for rules sets which are generated in this study to address the Conficker threat. The study also found that these worms rely completely on the infected computer to initiate any communication process in receiving any binary and payload from the author. Therefore, the rules set which are produced in this study will be focusing on preventing malicious traffic sent by infected computers to launch the communication process.

Keywords: malware, Conficker, malware analysis, Network Intrusion Detection and Prevention System

PENGENALAN

Penyediaan dan penggunaan perkhidmatan berasaskan atas talian oleh sesebuah organisasi sama ada jabatan kerajaan mahupun pihak swasta telah menunjukkan peningkatan yang amat ketara[1]–[3]. Penggunaan servis berkaitan perkomputeran awan di Malaysia juga mula menunjukkan peningkatan yang ketara terutamanya di dalam organisasi Kerajaan Malaysia seiring dengan inisiatif-inisiatif di bawah Program Transformasi Ekonomi (ETP), Bidang Ekonomi Utama Negara (NKEA) Perkhidmatan Perniagaan (*Business Services*), *EPP2-1 Government Shared Services* iaitu pelaksanaan projek Pusat Data Sektor Awam (PDSA) yang menyediakan perkhidmatan pusat data dan Pusat Pemulihan Bencana (DRC) bagi pengoperasian perkhidmatan ICT secara berpusat untuk agensi-agensi Kerajaan serta projek Perkhidmatan Komunikasi Bersepadu 1GovUC (termasuk emel, panggilan suara, faksimili, sidang video dan saluran komunikasi berasaskan internet yang lain) yang bertujuan untuk membantu memperkasa dan menambahbaik urusan komunikasi dan kolaborasi dalam urusan harian pentadbiran dan aktiviti utama agensi-agensi di dalam Sektor Awam melalui integrasi dan konsolidasi saluran-saluran komunikasi secara selamat [3]. //malaysia

Selaras dengan peningkatan terhadap permintaan dan penggunaan servis atas talian ini maka kebergantungan terhadap tahap ketersediaan dan keselamatan infrastrukur teknologi maklumat sesebuah organisasi (sama ada penyedia atau pengguna) adalah amat kritikal. Infrastuktur teknologi maklumat ditakrifkan sebagai satu set gabungan perkakasan, perisian, rangkaian, kemudahan, dan lain-lain yang diperlukan untuk membangun, menguji, menyampai, memantau, mengawal atau menyokong perkhidmatan perkhidmatan teknologi maklumat organisasi. Manusia (*people*), proses dan dokumentasi tidak termasuk dalam infrastruktur teknologi maklumat [4], [5]. Infrastrukur teknologi maklumat yang stabil dan selamat dapat memastikan aktiviti harian organisasi tidak terganggu disamping memastikan tahap keselamatan maklumat organisasi dalam keadaan yang terjamin. Ini kerana infrastrukur teknologi maklumat merupakan elemen terpenting dalam pelaksanaan servis atas talian kerana ianya sangat bergantung kepada perkongsian sumber (perkakasan atau perisian atau kedua-duanya) melalui medium sistem rangkaian komputer untuk mencapai kesepaduan dan tahap skala ekonomi terbaik [6], [7].//definisi infrstruktur IT

Seiring dengan peningkatan penggunaan perkhidmatan atas talian ini, ancaman keselamatan terhadap infrastrukur teknologi maklumat organisasi juga telah menunjukkan peningkatan yang ketara pada setiap tahun [8].Secara tidak langsung ianya memerlukan setiap organisasi memelihara tahap ketersediaan serta keselamatan aset teknologi maklumat sesebuah organisasi agar sentiasa berada dalam keadaan terbaik dan selamat. Antara ancaman keselamatan yang sering dihadapi oleh sesebuah organisasi terhadap aset maklumat mereka adalah perisian hasad yang mana ianya termasuklah virus, *trojan horse*, *worm* (Cecacing), *rootkit*, *scareware* dan *spyware* [9]. Kehadiran perisian hasad dalam organisasi amat berbahaya kerana boleh menyebabkan maklumat daripada sistem komputer hilang atau disekat malahan membolehkan segala aktiviti penggunaan di atas talian dipantau oleh penjenayah siber.

Cecacing merupakan ancaman yang mempunyai peratusan yang paling tinggi dari kumpulan perisian hasad. Berdasarkan laporan yang dikeluarkan oleh F-Secure sejak tahun 2012 sehingga 2014, ancaman cecacing Conficker telah menunjukkan peningkatan yang ketara [10]–[15]. Ketua Pegawai Eksekutif CyberSecurity Malaysia (Cybersecurity), Dr. Amirudin Abdul Wahab dipetik sebagai berkata bahawa ancaman perisian hasad pada rangkaian Internet di negara ini adalah amat serius yang mana antara perisian hasad tersebut adalah Cecacing Conficker [16]. Laporan oleh F-Secure (2014) turut menyatakan bahawa Malaysia merupakan salah sebuah daripada 5 buah negara penyumbang tertinggi dengan kedudukan kedua tertinggi di bawah UAE. Sehubungan dengan itu, kajian ini dijalankan bertujuan untuk mencapai dua objektif utama iaitu:

i. Menganalisa dan mengkaji gerak kerja semua varian Conficker seterusnya mengenalpasti laluan komunikasi yang digunakan oleh setiap varian dalam menerima sebarang binari atau muat beban;
ii. Merangka, menulis serta menguji set petua (*rules set*) sistem pengesanan dan pencegahan pencerobohan berasaskan rangkaian Snort untuk menangani ancaman Conficker.

KAJIAN LITERATUR

Bahagian ini menyoroti literatur mengenai ancaman keselamatan terhadap infrastruktur teknologi maklumat organisasi, perisian hasad serta Cecacing Conficker selain menerangkan jurang kajian sedia ada.

ANCAMAN KESELAMATAN

Ancaman dari sudut sistem maklumat ditakrifkan sebagai sebarang keadaan atau kejadian yang berpotensi untuk memberi kesan buruk kepada operasi organisasi (termasuk misi, fungsi, imej atau reputasi), aset organisasi atau

individu menerusi capaian yang tidak dibenarkan, kemusnahan, pendedahan, pengubahsuaian maklumat dan / atau penafian perkhidmatan terhadap sistem maklumat. Ianya juga termasuklah potensi sumber ancaman berjaya mengeksploitasi kelemahan sistem maklumat [17]. Seiring dengan perkembangan dan kebergantungan organisasi terhadap penggunaan teknologi maklumat serta peningkatan akses kepada Internet, menyebabkan sistem maklumat organisasi terdedah kepada serangan siber seterusnya akan mengakibat kerosakan terhadapnya. Oleh yang demikian, perenggan ini akan mengkaji dengan lanjut mengenai ancaman keselamatan terhadap infrastruktur teknologi maklumat.

Ancaman terhadap infrastruktur teknologi maklumat telah dibahagikan kepada tiga kelas utama iaitu manusia, persekitaran dan teknologi. Ancaman manusia merupakan ancaman akibat daripada tindakan yang boleh menyebabkan kerosakan dan risiko keselamatan terhadap sistem maklumat organisasi oleh orang dalam (kakitangan organisasi) serta serangan oleh penggodam. Manakala ancaman persekitaran pula adalah seperti bencana alam, huru-hara dan perang. Seterusnya dan yang terakhir adalah ancaman yang disebabkan oleh kegagalan perkakasan dan perisian termasuklah perkakasan sokongan yang mana ancaman ini dikelaskan sebagai ancaman teknologi. Semua kelas ancaman ini boleh hadir samada dari dalam atau luar organisasi. Walaubagaimanapun, tidak semua ancaman yang hadir merupakan ancaman hasad atau ditakrifkan sebagai ancaman yang bertujuan untuk mendatangkan kerosakan kepada sistem maklumat organisasi. Hanya ancaman dari kumpulan manusia sahaja yang mempunyai kemungkinan untuk melaksanakan ancaman hasad. Ancaman hasad boleh berlaku samaada dari luar atau pun dari dalam rangkaian organisasi yang disebabkan oleh kakitangan atau penggodam untuk merosak serta mengganggu organisasi seperti virus, kuda trojan, atau Cecacing (Jouini et al. 2014).

PERISIAN HASAD

Seringkali istilah seperti virus, cecacing, kuda trojan atau *rootkit* disebut dan dilaporkan apabila membincangkan perkara berkaitan keselamatan siber. Istilah-istilah ini menerangkan jenis program yang digunakan oleh penjenayah siber untuk menjangkiti dan mengambil alih komputer dan peranti mudah alih. Pada masa kini semua istilah yang berbeza ini digelarkan sebagai perisian hasad. Perisian hasad adalah istilah utama yang digunakan untuk merujuk kepada pelbagai bentuk perisian ganas atau mengganggu [18], [19]. Perisian hasad adalah merupakan gabungan perkataan hasad (*malicious*) dan perisian (*software*) yang mana ianya ditakrifkan sebagai sebarang perisian yang digunakan untuk menjejaskan fungsi serta operasi sistem komputer, mencuri data atau mendapatkan kawalan akses bagi memberikan kemudaratan kepada komputer hos [18], [19]. Ianya boleh wujud dalam bentuk kod boleh laku (*executable code*), skrip, kandungan aktif dan perisian lain. Perisian hasad sering menyamar seperti atau terdapat dalam fail yang tidak berniat jahat. Kaspersky Lab (2012) telah mengkelaskan perisian hasad kepada beberapa jenis utama antaranya adalah Cecacing, virus, *backdoor*, kuda *Trojan*, *rootkit* dan juga *exploit*. Sehingga 2011, majoriti ancaman perisian hasad aktif ialah cecacing atau *Trojan* dan bukan virus [19]. Kepelbagaian, kecanggihan dan kewujudan perisian hasad ini telah menimbulkan pelbagai cabaran yang besar terhadap pertahanan keselamatan rangkaian dan hos akhir (*end host*).

Perisian hasad boleh bersifat selinap (*stealth*), bertujuan untuk mencuri maklumat atau menghendap pengguna komputer untuk tempoh yang panjang tanpa pengetahuan mereka [13], [19] sebagai contohnya *Regin*, atau ia mungkin direka untuk menyebabkan kemudaratan dan sabotaj (contohnya *Stuxnet*), atau bagi tujuan memeras ugut (contohnya *CryptoLocker*). Terdapat juga perisian hasad lain yang ditemui tertanam dalam program-program rasmi yang dibekalkan oleh syarikat yang sah yang mana terdapat fungsi lain yang tersembunyi di dalam aplikasi tersebut sebagai contoh, fungsi pengesanan tambahan tersembunyi yang mengumpulkan statistik pemasaran. Contoh perisian seperti ini dan digambarkan sebagai tidak sah adalah *rootkit* oleh syarikat Sony [21]. Terdapat kuda *Trojan* yang tertanam ke dalam cakera padat muzik atau video yang dijual oleh pihak Sony, yang secara sembunyi dipasang dan menyembunyikan dirinya dalam komputer pembeli tanpa kebenaran mereka. Ianya berniat untuk menghalang penyalinan haram serta melaporkan tabiat mendengar pengguna dan secara tidak sengaja telah mencipta kelemahan yang boleh dieksploitasi oleh perisian hasad yang tidak berkaitan.

Matlamat akhir sebahagian besar penjenayah siber adalah untuk memasang perisian hasad ke dalam komputer atau peranti mudah alih sasaran [8], [11], [19], [22]. Setelah dipasang, penyerang ini berpotensi memperoleh kawalan sepenuhnya terhadap sasaran. Ramai yang mempunyai salah tanggapan bahawa perisian hasad hanya menyasarkan peranti yang menggunakan sistem pengoperasian Microsoft Windows sahaja. Walaupun sistem pengoperasian ini digunakan secara meluas seterusnya menjadikan ianya sebagai sasaran terbesar, perisian hasad tetap boleh menjangkiti mana-mana peranti pengkomputeran, termasuk telefon pintar dan tablet yang menggunakan sistem pengoperasian lain. Malah, kelaziman perisian berniat jahat menjangkiti peranti mudah alih semakin berkembang [8], [10]. Semakin banyak komputer dan peranti mudah alih berjaya dijangkiti oleh penjenayah siber, semakin banyak keuntungan yang boleh mereka perolehi. Penjenayah ini biasanya tidak peduli siapa yang mereka jangkiti asalkan mereka berjaya menjangkiti seberapa ramai orang yang mungkin.

Perisian hasad tidak lagi dicipta sebagai hobi atau oleh penggodam amatur, tetapi oleh penjenayah siber yang canggih dengan niat untuk membantu mereka mencapai matlamat tertentu. Matlamat ini boleh termasuk mencuri data sulit, penuaian maklumat pengguna dan kata laluan, menghantar e-mel spam, melancarkan serangan penafian perkhidmatan, peras ugut atau kecurian identiti. Sebagai contoh, perisian yang dikenali sebagai *Cryptolocker* digunakan oleh penjenayah siber untuk menjangkiti dan menyulitkan semua fail pada komputer anda. Setelah dijangkiti dan disulitkan, penjenayah siber kemudian menuntut wang tebusan sebagai pertukaran untuk menyahsulit semula fail anda [8], [10], [11], [19].

Mereka yang mencipta, menggunakan dan mendapat manfaat daripada perisian hasad boleh terdiri daripada individu-individu yang bertindak sendiri, untuk kumpulan jenayah yang terancang atau organisasi kerajaan [23]. Di samping itu, mereka yang mencipta perisian hasad yang canggih pada hari ini kebiasaanya sangat berdedikasi terhadap tujuan mereka. Malahan penciptaan perisian hasad merupakan pekerjaan sepenuh masa mereka. Apabila mereka berjaya membangunkan perisian hasad, mereka sering menjualnya kepada individu atau organisasi lain serta menyediakan program kemaskini yang teratur dan khidmat sokongan kepada pelanggan mereka. Setelah dibeli, pelanggan atau penjenayah lain akan mendapatkan keuntungan melalui pemasangan perisian hasad ke dalam berjuta-juta sistem mangsa yang dijangkiti untuk mewujudkan Rangkaian Bot (*botnet*). Rangkaian Bot ini menjadi tentera yang dikawal dari jarak jauh oleh penjenayah siber untuk kegunaan mereka sendiri, atau menjualnya kepada penjenayah siber yang lain [22].

Apabila penyerang berada di bahagian dalam sesebuah sistem rangkaian organisasi, kerjanya adalah jauh lebih mudah kerana kebanyakan rangkaian dan sistem di bahagian dalam akan lebih dipercayai. Inilah yang membuatkan, dengan menyerang pelawat web melalui laman web yang dijangkiti, begitu menarik dan mudah untuk penjenayah. Ini kerana pengguna akhir dan pelayar web sudah berada di dalam rangkaian dalaman. Tidak seperti serangan berasaskan rangkaian tradisional, mangsa yang akan menghubungi penyerang dan bukan sebaliknya [24]. Malahan pada hari ini, kebanyakan sistem pertahanan masih memberi tumpuan kepada menghalang penyerang daripada mencuba untuk menyambung kepada mangsa contohnya dengan melindungi perimeter berbanding menghalang pengguna dalaman menghubungi penjenayah. Perisian hasad akan memberikan ancaman keselamatan terhadap keselamatan maklumat organisasi terutamanya dari sudut kerahsiaan, keutuhan dan ketersediaan aset dan maklumat organsasi. Secara tidak langsung ianya boleh memberikan kerugian terhadap organisasi bukan sahaja dari sudut kewangan malahan dari sudut masa, tenaga kerja serta produktiviti selain daripada mencalar reputasi organisasi.

CECACING CONFICKER

Pada 23 Oktober 2008, pihak Microsoft telah mengeluarkan buletin keselamatan yang mempunyai tahap kritikal iaitu MS08-067 - *Vulnerability in Server Service Could Allow Remote Code Execution* (958644)[25]. Buletin tersebut telah menjelaskan berkaitan kelemahan (*vulnerability*) yang terdapat dalam perkhidmatan pelayan. Kelemahan ini boleh membenarkan pelaksanaan kod arahan secara jarak jauh jika sistem yang terjejas menerima permintaan prosedur panggilan jarak jauh (*Remote Procedure Call*) yang direka secara khusus. Ini boleh membenarkan penyerang untuk mengeksploitasi kelemahan ini (tanpa memerlukan melalui sebarang proses pengesahan ketulenan) untuk melaksanakan atau melarikan sebarang kod terhadap sistem pengoperasian yang terjejas. Antara versi Microsoft Windows yang terkesan dengan kelemahan ini adalah Windows XP, Windows Vista, Windows 7 beta, Windows Server 2000, Windows Server 2003 dan Windows Server 2008.

Buletin ini juga telah memberikan amaran bahawa kelemahan ini mempunyai potensi untuk digunakan sebagai mekanisme tunggal untuk penyebaran (Nazario, Ptacek, & Song, 2004) dan eksploitasi cecacing. Kelemahan yang juga dirujuk sebagai CVE-2008-4250 (CVE, 2008) telah diberikan tahap rating tertinggi iaitu 10.0 oleh *Common Vulnerability Scoring System* (CVSS) (US-CERT/NIST, 2012) untuk menunjukkan bahawa kelemahan ini berimpak tinggi serta berpotensi tinggi untuk dieksploitasi. CVSS adalah sistem pemarkahan yang direka untuk menyediakan satu kaedah yang terbuka dan seragam bagi penarafan tahap sesuatu kelemahan dalam bidang teknologi maklumat (terutamanya kelemahan berkaitan perisian).

Pada November 2008, satu jenis cecacing telah dikesan mengeksploitasi kelemahan yang terdapat pada sistem pengoperasian Microsoft Windows ini. Cecacing ini telah dikenali sebagai Conficker. Ianya juga dikenali sebagai '*Downup*', '*Downadup*' atau *'Kido'* oleh pelbagai pihak pengeluar AntiVirus (Kaushik, 2013).Ancaman oleh perisian hasad daripada jenis Cecacing merupakan ancaman yang paling berbahaya terhadap organisasi berbanding ancaman perisian hasad dari jenis lain kerana ianya tergolong di dalam kumpulan Cecacing jenis *Net-Worm* dan diklasifikasi sebagai keluarga *Net-Worm.Win32.Kido* [20]. Cecacing yang berada di bawah kumpulan ini merupakan perisian hasad yang paling berbahaya dan memberikan ancaman yang serius terhadap keselamatan aset maklumat organisasi. Cecacing ini berkeupayaan untuk menamatkan, melumpuhkan, menyusun semula atau mewujudkan lubang hitam terhadap sistem pengoperasian dan perkhidmatan keselamatan pihak ketiga (Porras et al. 2009). Conficker akan melumpuhkan perkhidmatan keselamatan sistem operasi Windows, perisian tembok api (*firewall*) pihak ketiga dan juga produk anti-virus dengan melumpuhkan

kemaskini secara automatik. Ianya bukan sahaja memberikan masa untuk ianya merebak, tetapi boleh menyediakan satu tapak untuk perisian hasad lain maka memburukkan lagi masalah keselamatan organisasi.

Tujuan utama Conficker adalah untuk mengambil alih kawalan sepenuhnya terhadap komputer yang telah dijangkiti dengan menyediakan mereka perkhidmatan kemas kini binari yang selamat (melalui teknologi kriptografi) bagi membenarkan penulisnya mengawal berjuta-juta komputer di seluruh dunia yang telah dijangkiti (Porras et al. 2009). Setiap muat beban (*payload*) atau kemaskini yang dihantar akan menggunakan penyulitan binari, teknologi enkripsi dan tandatangan digital yang mana hanya penulisnya sahaja yang mempunyai kunci tersebut (Nahorney 2009). Pelbagai pihak membuat kesimpulan bahawa matlamat paling mungkin terhadap penciptaan dan penyelenggaraan platform berskala besar Conficker dipercayai untuk pengedaran perisian berasaskan jenayah. Ini disokong oleh muat beban yang dipasang dalam varian A dan varian E serta insiden yang berlaku pada bulan Jun 2011 di mana satu kumpulan penjenayah di Ukraine telah ditangkap kerana menggunakan Conficker untuk mengagihkan muat beban *phishing* kepada beberapa buah bank [27], [28]. Charles & Shari (2012) menyatakan bahawa Conficker telah digunakan untuk pelakuan jenayah dengan menyediakan platform kepada serangan *Spam* dan pengiklanan anti virus palsu bagi tujuan keuntungan kewangan. Rekabentuk Conficker membolehkan ianya digunakan untuk tujuan sabotaj, serangan DDoS, pemusnahan data, kecurian harta intelek serta apa saja tujuan dengan syarat muat bebannya ditandatangani oleh penulisnya [29].

Jadual 1 Jadual penamaan varian Conficker
Sumber : (Irwin 2012)

Tarikh	Microsoft	Conficker Working Group (CWG)
20 Nov 2008	Conficker.A	Conficker.A
28 Dis 2008	Conficker.B	Conficker.B
20 Feb 2009	Conficker.C	Conficker.B++
4 Mac 2009	Conficker.D	Conficker.C
8 Apr 2009	Conficker.E	Conficker.E

Jadual 1 di atas menunjukkan perbezaan dalam penamaan untuk setiap varian Cecacing Conficker terutamanya setelah muncul varian ketiga selepas varian B. Kekurangan skim penamaan yang sama untuk Conficker dan perselisihan di kalangan penganalisis dalam mengeluarkan penamaan untuk varian baru agak menyukarkan. Sebagai contoh, varian ketiga iaitu varian B++ oleh Kumpulan Kerja Conficker (CWG) adalah sama dengan varian C pada Microsoft dan varian C (CWG) bersamaan dengan varian D (Microsoft). Ini kerana, pihak CWG menyatakan bahawa varian ketiga yang dijumpai pada 20 Feb 2009 adalah merupakan perubahan kecil terhadap varian B sedia ada. Manakala, pihak Microsoft telah meletakkannya sebagai varian C dengan alasan varian tersebut tetap berbeza dengan varian B tanpa mengira perubahan kecil atau perubahan yang ketara. Untuk tujuan kegunaan dalam kajian ini, penamaan varian akan dirujuk menggunakan penamaan oleh Microsoft.

Cecacing Conficker merupakan satu ancaman bercampur kerana ianya boleh tersebar melalui pelbagai sumber dan medium [30] antaranya adalah dengan mengekploitasi kelemahan MS08-067, MS08-068 dan MS09-01, menggunakan kelemahan fungsi Autorun (*USB disk / CD / External Drive*), melalui perkongsian rangkaian (*network share*) serta kelemahan katalaluan. Shin et al. (2012) telah mengkaji bahawa Conficker lebih berkemungkinan untuk menjangkiti hos yang terdekat berbanding secara rawak. Ianya menggunakan lebih daripada satu strategi penyebaran [32] iaitu Penerokaan Tempatan (*Local probing*), Penerokaan Kejiranan (*Neighbourhood probing*) dan Penerokaan Sejagat (*Global probing*.

JURANG KAJIAN

Berasaskan kepada *Business Model for Information Security* (BMIS) yang dibangunkan oleh Dr. Laree Kiely and Terry Benzel, terdapat empat entiti utama empat entiti utama iaitu organisasi, teknologi, proses dan manusia dalam menangani ancaman keselamatan terhadap keselamatan maklumat organisasi [33]. Walaubagaimanapun, kajian ini hanya akan memberikan tumpuan terhadap kaedah pertahanan yang berada di bawah entiti teknologi dalam menangani ancaman keselamatan ini. Dalam menangani ancaman Conficker terhadap infrastruktur maklumat organisasi, ianya boleh diimplementasi kepada dua titik utama yang terlibat iaitu:

i. Komputer atau perkakasan yang dijangkiti;
   Kaedah pertahanan paling mapan dan terbaik dalam menangani ancaman Conficker adalah dengan melaksanakan tindakan pembersihan dan pencegahan terhadap semua komputer, pelayan dan perkakasan

dalam sistem rangkaian organisasi yang telah dijangkiti atau tidak. Antaranya memasang tampalan, mematikan fungsi Autoplay, katalaluan yang kukuh, kawalan hak akses minimal dan mengemaskini perisian anti-virus [26], [34]–[36].

ii. Pelayan Arahan dan Kawalan Conficker;

Selain daripada pelaksanaan kaedah pertahanan diperingkat hos komputer dalam rangkaian, terdapat juga kajian berkaitan kaedah pertahanan dilapisan rangkaian yang bertujuan untuk menghalang trafik daripada komputer yang dijangkiti dari menghubungi pelayan arahan dan kawalan. Antonakakis et al. (2010) telah mengkaji kaedah pertahanan pada lapisan rangkaian terhadap cecacing Conficker dengan menggunakan kaedah Sistem Reputasi Dinamik untuk DNS[37]. Sistem pertahanan ini menggunakan kaedah senarai hitam terhadap senarai nama domain yang dikenalpasti sebagai berkait dengan cecacing Conficker. Kaedah ini dilaksanakan dengan cara memecahkan algoritma penjanaan domain oleh Conficker seterusnya mendaftar nama domain yang akan digunakan oleh hos arahan dan kawalan Conficker[31]. Ianya bagi menghalang penulis / pemilik Conficker berhubung dengan sistem yang telah dijangkiti.

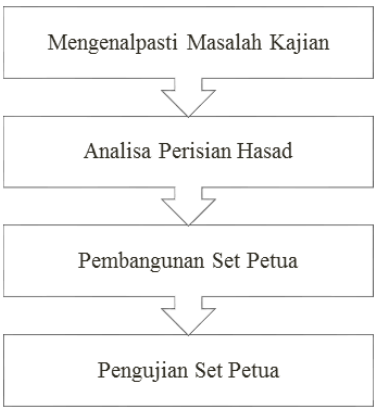
Walaupun pelaksanaan tindakan pencegahan dan pembersihan diperingkat hos komputer dalam rangkaian organisasi merupakan kaedah terbaik dan paling mampan dalam menangani ancaman Conficker, tetapi ia merupakan kaedah pertahanan yang paling rumit untuk dilaksanakan oleh organisasi terutamanya yang bersaiz besar. Kaedah ini mungkin sesuai jika bilangan komputer yang terdapat di dalam sesebuah organisasi tersebut adalah kecil serta saiz sistem rangkaian yang ringkas. Jika saiz sistem maklumat dan rangkaian sesebuah organisasi itu besar, maka ianya akan melibatkan kos yang sangat tinggi terutamanya dari segi kos buruh, kepakaran, masa serta kos operasi.

Oleh yang demikian, daripada bergantung kepada penyelesaian secara setempat ini, kerumitan ini boleh dikurangkan dengan terus menyepadukan kaedah pertahanan keselamatan ke dalam fabrik rangkaian itu sendiri (Wadner & Atlasis, 2013). Ianya memberi kelebihan dari segi memantau dan menganalisis fail secara berterusan serta mengenal pasti tingkah laku yang berniat jahat berikutnya setiap kali ia mungkin bermula (Cisco, 2014). Walaubagaimanapun, berdasarkan kepada kajian yang dilaksanakan oleh (Shin et al. 2012) telah menemui kelemahan dalam kaedah pertahanan menggunakan senarai hitam nama domain pelayan arahan dan kawalan dalam menangani ancaman Conficker seperti Sistem Reputasi Dinamik untuk DNS. Kaedah ini memerlukan usaha dan kerjasama yang amat tinggi oleh semua pihak terutamanya pihak TLD (*Top Level Domain*) serta ianya memerlukan kos yang amat tinggi untuk dilaksanakan [38]. Oleh yang demikian, perlu ada satu kaedah terbaik di lapisan rangkaian yang perlu disediakan dalam menangani ancaman Conficker ini terhadap keselamatan infrastruktur maklumat organisasi.

Mehmood et al. (2013), Modil et al. (2012), S. Shin et al. (2012), Simmons et al. (2009) dan Waskita et al. (2014) telah mencadangkan bahawa penggunaan kaedah pertahanan menggunakan sistem pengesanan dan pencegahan pencerobohan di lapisan rangkaian merupakan kaedah paling berkesan dalam memelihara tahap keselamatan infrastrukur teknologi maklumat organisasi[31], [39]–[42]. Sistem ini berfungsi dengan memantau semua trafik dalam rangkaian organisasi seterusnya mengesan serta menghalang sebarang pencerobohan serta sebarang aktiviti yang mencurigakan.

METODOLOGI KAJIAN

RANGKA KERJA KAJIAN



Rajah 1 Rangka Kerja Kajian

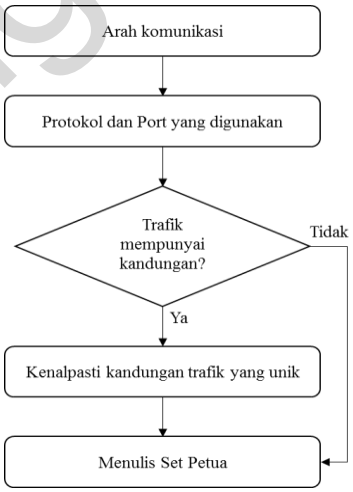
Kajian ini dilaksanakan dalam empat peringkat bermula dari proses mengenalpasti masalah kajian sehinggalah proses pengujian terhadap hasil kajian melalui proses eksperimen bagi menentusahkan hasil kajian.Fasa

mengenalpasti masalah kajian ini telah dilaksanakan melalui kaedah kajian kesusasteraan secara bersistematik. Ianya dilaksanakan berdasarkan pembacaan serta analisis kritikal terhadap buku-buku berkaitan, jurnal, artikel, kertas kerja seminar dan penyelidikan, tesis-tesis pengkaji terdahulu, akbhar serta artikel dari laman web terkenal yang berkaitan dengan keselamatan maklumat. Fasa ini penting dalam memberi kefahaman mengenai bidang kajian dan menjadi panduan penyelidikan. Secara umumnya, kajian kesusasteraan dalam fasa ini telah dilaksanakan secara dua peringkat bagi dua penghasilan yang berbeza.

Peringkat pertama kajian kesusasteraan dilaksanakan bagi tujuan mengenalpasti serta memahami dengan lebih lanjut mengenai isu yang timbul dalam bidang kajian yang dilaksanakan seterusnya menjadi penggerak dalam penghasilan kajian ini. Hasil kajian peringkat pertama ini membantu dalam mengenal pasti bidang yang hendak dikaji, corak semasa subjek kajian dan seterusnya mengenal pasti jurang yang wujud dan apakah yang sepatutnya dicapai oleh kajian ini.Manakala, peringkat kedua dalam kajian kesusasteraan yang dilaksanakan dalam fasa ini menumpukan sepenuhnya kepada skop dan objektif berkaitan dengan subjek kajian yang telah dihasilkan pada peringkat pertama. Ia bertujuan untuk mengkaji dengan lebih mendalam berkaitan subjek kajian seterusnya mendapatkan gambaran awal mengenai ancaman yang dihadapi bagi membantu proses penyediaan kaedah yang sesuai untuk menangani ancaman tersebut.

Seterusnya merupakan fasa pelaksanaan analisa terhadap Cecacing Conficker. Secara umumnya, aktiviti dalam fasa ini merujuk kepada metodologi analisa perisian hasad yang dibangunkan oleh Micheal Sikorsky dan Andrew Honig melalui bukunya yang bertajuk *Practical Malware Analysis* sebagai asas. Bagaimanapun, kaedah oleh Sikorsky dan Honig ini hanya dijadikan sebagai asas rujukan utama dalam membangunkan fasa ini dan fasa yang seterusnya dalam metodologi kajian ini bagi menyesuaikan dengan perisian hasad yang dianalisa serta kaedah pertahanan yang akan digunakan. Maklumat dan kesimpulan yang diperolehi dalam fasa ini akan menjadi input penting terhadap fasa seterusnya iaitu dalam pembangunan set petua. Ini kerana dalam membangunkan set petua yang berkesan dalam menangani ancaman Conficker, maklumat dan pengetahuan yang mendalam terhadap perisian hasad yang dikaji adalah merupakan perkara yang sangat penting untuk diambil perhatian [9].

Fasa pembangunan set petua ini merupakan proses untuk menghasilkan set petua bagi kegunaan sistem pengesanan dan pencegahan pencerobohan Snort. Proses pembangunan set petua dalam fasa ini akan dilaksanakan dengan melaksanakan analisa dinamik terhadap data trafik rangkaian yang telah direkodkan ketika pelaksanaan fasa dua sebelum ini. Berbeza dengan analisa dinamik yang telah dilaksanakan dalam fasa 2 yang mana lebih menumpukan kepada corak trafik rangkaian, analisa terhadap data trafik rangkaian dalam fasa ini lebih menumpukan kepada kandungan dalam setiap transaksi rangkaian yang berkaitan.Tujuan analisa kandungan trafik rangkaian ini adalah untuk melihat ciri-ciri penting yang perlu dimasukkan ke dalam set petua bagi tujuan semakan oleh sistem pengesanan pencerobohan ini. Secara umumnya, pelaksanaan fasa ini seperti yang ditunjukkan di dalam Rajah 2 di bawah.



Rajah 2 Carta Alir Pembangunan Set Petua

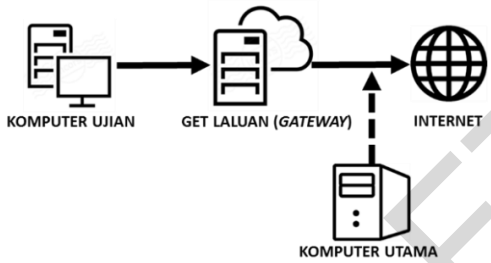
Fasa terakhir dalam kajian ini adalah pengujian terhadap set petua yang dihasilkan dalam fasa sebelum ini melalui proses eksperimen. Ianya bertujuan untuk menentusahkan setiap set petua yang dibangunkan. Ianya bagi memastikan setiap set petua yang dihasilkan dalam kajian ini berjaya mencapai matlamat kajian ini iaitu menghalang komunikasi di antara penulis Conficker dengan mangsanya. Bagi melaksanakan proses pengujian terhadap set petua dalam fasa ini, terdapat dua persekitaran ujian yang disediakan iaitu Persekitaran Kawalan dan Persekitaran Rawatan. Persekitaran kawalan merupakan persekitaran asas dalam kajian ini yang mana ianya akan dijadikan sebagai rujukan terhadap data trafik rangkaian yang telah dijangkiti oleh cecacing Conficker

tanpa sebarang mekanisma pertahanan. Manakala Persekitaran Rawatan pula adalah persekitaran ujian yang mempunyai mekanisma pertahanan yang mana dalam kajian ini, mekanisma pertahanan tersebut adalah sistem pengesanan dan pencegahan pencerobohan Snort yang telah dipasangkan dengan set petua yang dibangunkan dalam fasa ketiga kajian ini. Dalam fasa ini, data yang diperolehi melalui Persekitaran Rawatan (Data Rawatan) akan dibandingkan dengan data yang diperolehi melalui Persekitaran Kawalan (Data Trafik Kawalan) serta data yang diperolehi dari laporan Kotak Pasir mengikut kumpulan varian bagi melihat keberkesanan set petua yang dibangunkan dalam menghalang sebarang komunikasi yang dihasilkan oleh semua varian Conficker.

PERSEKITARAN EKSPERIMEN

Dalam melaksanakan proses analisa perisian hasad serta pembangunan dan pengujian set petua dalam kajian ini, beberapa persekitaran eksperimen telah diwujudkan bagi menyokong matlamat kajian. Persekitaran yang diwujudkan dalam kajian ini adalah seperti berikut:

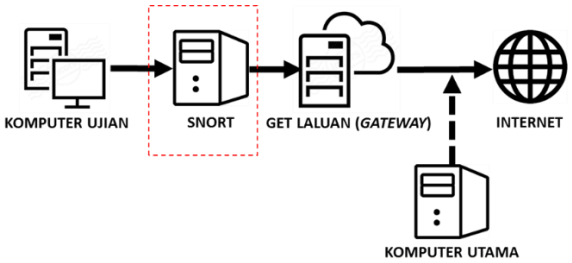
i. Persekitaran Kawalan



Rajah 3 Persekitaran Kawalan

Terdapat lima Persekitaran Kawalan yang diwujudkan dalam kajian ini. Ianya adalah bagi mewakili lima varian cecacing Conficker. Setiap Persekitaran Kawalan yang mewakili setiap varian akan mempunyai 5 buah set Komputer Ujian yang akan dilarikan pada waktu dan tarikh yang berbeza tetapi mempunyai tempoh yang sama bagi menghasilkan 5 set sampel data trafik kawalan. Dalam persekitaran ini Komputer Ujian perlu melalui pelayan get laluan sebelum mencapai akses ke internet. Pelayan get laluan dalam eksperimen ini akan menggunakan sistem pengoperasian *pfsense* (berasaskan *freeBSD* Linux). Ianya berfungsi sebagai penghala rangkaian disebabkan oleh segmen rangkaian yang berbeza digunakan oleh Komputer Utama berbanding Komputer Ujian. Komputer Utama pula akan berada di dalam segmen rangkaian yang sama dengan segmen IP luaran pelayan get laluan. Ini kerana Komputer Utama ini akan melaksanakan penghiduan terhadap trafik rangkaian dari get laluan ke internet. Kaedah yang digunakan dalam merekod trafik rangkaian ini adalah menggunakan perisian Wireshark dan mengkonfigur antaramuka rangkaian Komputer Utama dalam mod rambang. Setiap trafik rangkaian yang melalui get laluan serta menghala ke internet akan di rekodkan oleh Komputer Utama. Setiap data trafik rangkaian yang dijana dalam Persekitaran Kawalan ini akan direkodkan oleh Komputer Utama dan ditandakan sebagai Data Trafik Kawalan.

ii. Persekitaran Rawatan



Rajah 4 Persekitaran Rawatan

Seperti Persekitaran Kawalan, terdapat lima Persekitaran Rawatan yang diwujudkan dalam kajian ini. Ianya adalah bagi mewakili lima varian cecacing Conficker. Setiap Persekitaran Rawatan yang diwujudkan bagi mewakili setiap varian akan mempunyai 5 buah set Komputer Ujian yang akan dilarikan pada waktu dan tarikh yang berbeza tetapi mempunyai tempoh yang sama bagi menghasilkan 5 set sampel data trafik rawatan. Dalam Persekitaran Rawatan ini Komputer Ujian perlu melalui pelayan get laluan sebelum mencapai akses ke internet. Pelayan get laluan dalam eksperimen ini akan menggunakan sistem

pengoperasian *pfsense* (berasaskan *freeBSD* Linux). Ianya berfungsi sebagai penghala rangkaian disebabkan oleh segmen rangkaian yang berbeza digunakan oleh Komputer Utama berbanding Komputer Ujian. Komputer Utama pula akan berada di dalam segmen rangkaian yang sama dengan segmen IP luaran pelayan get laluan. Ini kerana Komputer Utama ini akan melaksanakan penghiduan terhadap trafik rangkaian dari get laluan ke internet. Kaedah yang digunakan dalam merekod trafik rangkaian ini adalah sama seperti yang digunakan dalam Persekitaran Kawalan iaitu menggunakan perisian Wireshark dan mengkonfigur antaramuka rangkaian Komputer Utama dalam mod rambang. Setiap trafik rangkaian yang melalui get laluan serta menghala ke internet akan di rekodkan oleh Komputer Utama. Komponen yang berada dalam Persekitaran Rawatan adalah hampir sama seperti Persekitaran Kawalan kecuali dalam persekitaran ini, komponen sistem pengesanan dan pencegahan pencerobohan Snort akan ditambah dalam diagram rangkaian Perisian Snort yang digunakan dikonfigur secara dalam baris (*inline*). Ini kerana ianya akan bertindak sebagai sistem pengesanan dan pencegahan pencerobohan dalam persekitaran ini bagi menghalang semua trafik hasad yang dikaji. Set petua yang telah dibangunkan dalam fasa ketiga sebelum ini akan dimasukkan ke dalam konfigurasi modul Snort. Seterusnya, proses pengujian terhadap Komputer Ujian yang telah dijangkiti oleh setiap varian Conficker akan dilaksanakan.

Bagi memastikan data trafik yang direkodkan tidak terganggu oleh faktor masa, persekitaran dan jangkitan di antara Komputer Ujian, pada setiap sesi pengujian hanya satu Komputer Ujian (mengikut varian yang ingin diuji) sahaja yang akan dihidupkan. Selain itu, komponen dalam kedua-dua persekitaran iaitu kawalan dan rawatan akan dihidupkan secara serentak serta Komputer Ujian yang digunakan juga akan menggunakan petikan imej yang sama. Begitu juga dengan Komputer Utama yang mana ianya mempunyai konfigurasi yang sama dalam kedua-dua persekitaran. Perbezaan yang terdapat dalam kedua-dua persekitaran ini hanyalah dari segi konfigurasi alamat IP untuk setiap komponen. Ini adalah kerana kedua-dua persekitaran ini akan dihidupkan dan dilarikan secara serentak. Bagi mengelakkan berlaku pertindihan rangkaian serta jangkitan di antara varian melalui rangkaian, maka semua komponen dalam Persekitaran Rawatan ini diletakkan dalam segmen rangkaian yang berbeza dengan Persekitaran Kawalan. Setiap data trafik rangkaian yang dijana dalam Persekitaran Rawatan ini akan direkodkan oleh Komputer Utama dan dilabelkan sebagai Data Trafik Rawatan.

iii. Persekitaran Kotak Pasir (*Sandbox*)

Kotak pasir adalah satu platform keselamatan yang disediakan untuk melarikan dan melaksanakan fail boleh laku yang tidak diketahui atau bersifat hasad di dalam persekitaran khusus tanpa mendatangkan risiko serta memberi kesan kepada sistem [43]. Pada asasnya, kotak pasir adalah persekitaran maya yang mensimulasikan persekitaran sistem sebenar untuk memastikan fail boleh laku yang diuji berjalan dengan cara yang hampir sama (jika tidak serupa) dengan kelakuannya dalam persekitaran sebenar. Ianya digunakan bagi menganalisis tingkah laku mereka (fail hasad yang dikaji) serta memberi maklumat berkaitan dengan kajian yang dilaksanakan [44]–[47].Sistem kotak pasir membolehkan pemantauan terhadap fail boleh laku yang mencurigakan dilaksanakan dalam persekitaran yang terpencil dan mengurangkan risiko menjejaskan sistem secara langsung. Satu lagi aspek penting ialah sistem kotak pasir ialah mengurangkan tugasan yang kompleks dan panjang seperti merungkai serta menyahkod fail yang berkaitan dengan perisian hasad untuk memahami tujuandan kelakuannya. Beberapa kajian telah mendapati bahawa penggunaan persekitaran kotak pasir dalam melaksanakan analisis dan pengujian terhadap fail berkaitan perisian hasad kerap memberikan hasil yang lebih baik berbanding menggunakan persekitaran lain [48], [49].Kajian ini menggunakan dua persekitaran Kotak Pasir iaitu perkhidmatan beberapa buah kotak pasir secara atas talian dan juga secara tempatan menggunakan perisian Cuckoo.

DAPATAN KAJIAN

MEDIUM KOMUNIKASI

Jadual 2 Medium Komunikasi Conficker

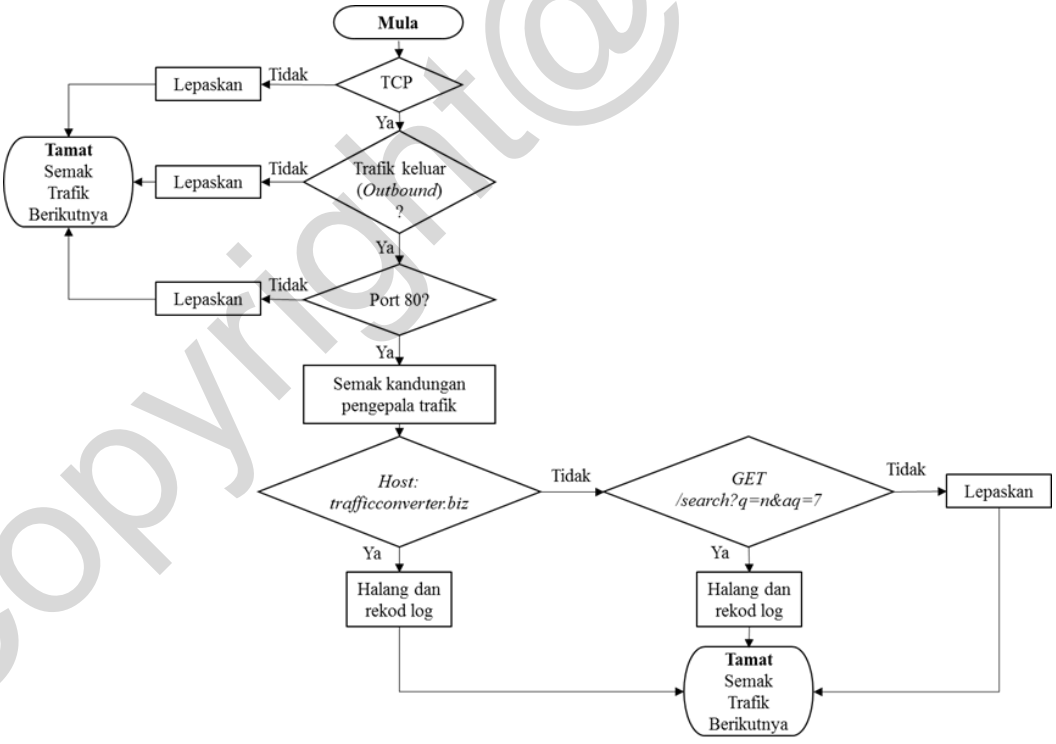
VARIAN (tarikh dikesan)	**MEDIUM KOMUNIKASI**		**DOMAIN DIHUBUNGI / DIJANA**	**BIL. TLD**
	TITIK PERTEMUAN (HTTP)	**PERANGKAI PADANAN (P2P)**		
A (20/11/2008)	√ tcp (≥1024) →tcp (80)	-	250 / 250	5
B (28/12/2008)	√ tcp (≥1024) →tcp (80)	-	250 / 250	8

C (20/2/2009)	√ tcp (≥1024) →tcp (80)	-	250 / 250	8
D (4/3/2009)	√ tcp (≥1024) →tcp (80)	√ udp (≥1024) →udp(≥1024)	500 / 50,000	110
E (8/4/2009)	√ tcp (≥1024) →tcp (80)	-	500 / 50,000	8

Berdasarkan kepada Jadual 2 di atas, semua varian Conficker menggunakan Titik Pertemuan sebagai medium komunikasi dalam menerima sebarang muat turun daripada penulisnya. Walaubagaimanapun, Varian D mempunyai laluan alternatif terhadap proses komunikasi ini yang mana ianya menggunakan protokol perangkai padanan untuk melaksanakan proses penerokaan pelayan dan pelanggan dalam rangkaian komunikasinya serta menggunakan protokol TCP untuk menghantar atau menerima sebarang muatbeban. Bilangan domain yang dijana dan dihubungi oleh varian D dan E bagi mekanisma Titik Pertemuan menunjukkan penambahan yang ketara terutamanya varian D yang menggunakan sehingga 110 TLD dalam janaan nama domain. Keadaan ini telah menambahkan tahap kesukaran untuk pihak CWG menyenarai hitam domain yang berkaitan dengan cecacing Conficker.

CARTA ALIR SEMAKAN CIRI UNIK TRAFIK SETIAP VARIAN

Kajian yang dilaksanakan telah menghasilkan carta alir dalam melaksanakan semakan terhadap setiap paket trafik bagi mengesan sebarang kehadiran komunikasi Conficker terhadap Titik Pertemuan dan Perangkai Padanan seterusnya menghalangnya daripada melepasi Sistem Pengesanan dan Pencegahan Pencerobohan. Carta alir ini membantu dalam pembangunan dan penghasilan set petua dalam kajian ini serta boleh digunakan dalam kaedah pertahanan lain. Carta alir yang dihasilkan mengikut varian Conficker adalah seperti berikut :

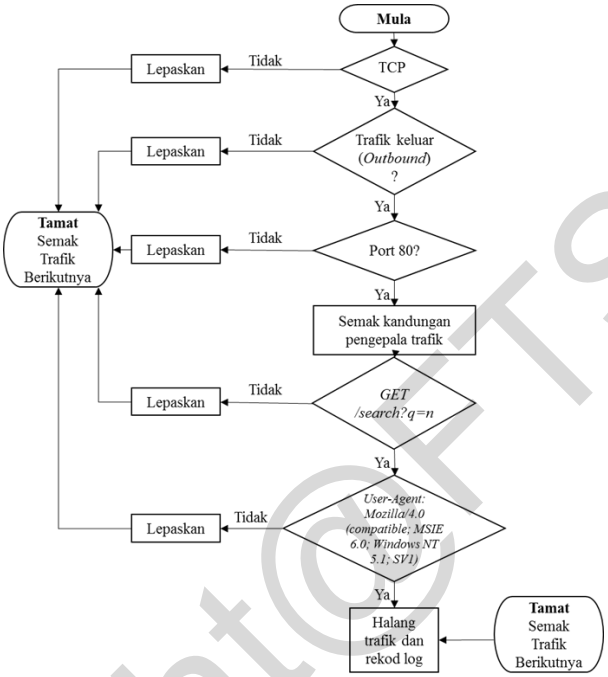


Rajah 5 Carta Alir Semakan Pengesanan Trafik Komunikasi Varian A

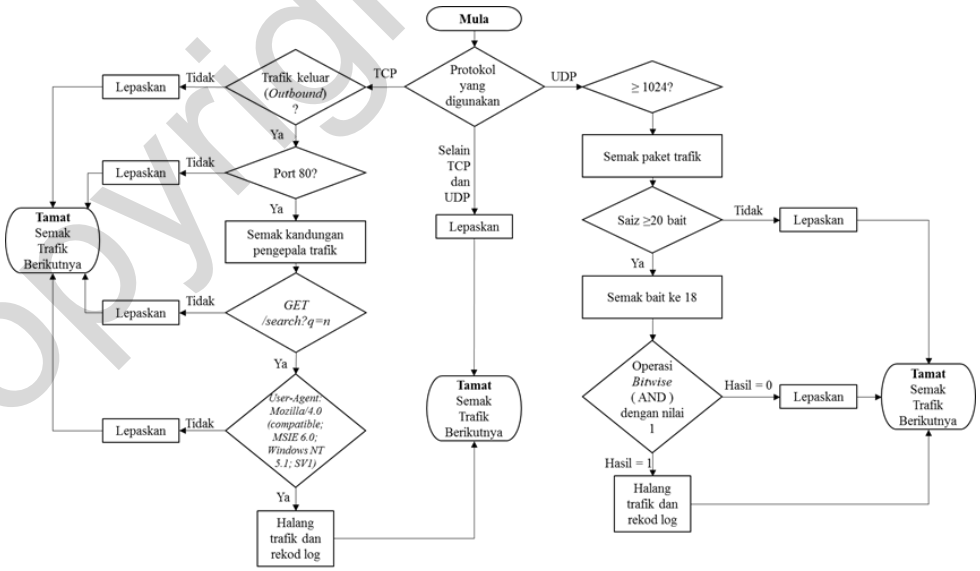
Rajah 5 di atas menunjukkan carta alir semakan yang dilaksanakan dalam menghalang sebarang perhubungan komputer yang telah dijangkiti dengan pelayan *trafficconverter.biz* dan juga dengan semua domain Titik Pertemuan yang dijana. Ianya akan menghalang paket trafik yang memenuhi syarat dalam carta alir di atas bagi tujuan menghalang sebarang komunikasi hasad yang berkaitan dengan Conficker A daripada diproses. Conficker varian B, C dan E mempunyai ciri unik yang sama. Oleh yang demikian, carta alir yang digunakan untuk mengesan kehadiran paket trafik ketiga-tig varian ini menggunakan aliran semakan yang sama (Rajah 6).

Rajah 7 pula menunjukkan aliran semakan dalam mengesan dan menghalang proses komunikasi oleh komputer yang dijangkiti oleh Conficker varian D. Varian ini mempunyai aliran semakan yang sama seperti

varian B, C dan E bagi semakan paket trafik ke Titik Pertemuan (menggunakan protokol TCP, port 80). Walaubagaimanapun, varian ini mempunyai tambahan dalam aliran semakannya kerana varian ini turut menggunakan mekanisma Perangkai Padanan dalam proses komunikasinya. Berbeza dengan aliran semakan terhadap trafik yang berkaitan dengan komunikasi Titik Pertemuan yang hanya menumpukan kepada semua paket keluar (*outbound*), semakan terhadap trafik yang melalui Sistem Pengesanan dan Pencegahan Pencerobohan menggunakan protokol UDP akan disemak dari kedua-dua arah iaitu *inbound* dan *outbound*. Ini kerana mekanisma perangkai padanan ini digunakan oleh varian ini untuk proses penerokaan terhadap pelayan dan juga pelanggan yang berada di luar rangkaian organisasi dalam menerima dan menghantar muatbeban.



Rajah 6 Carta Alir Semakan Pengesanan Trafik Komunikasi Varian B, C dan E



Rajah 7 Carta Alir Semakan Pengesanan Trafik Komunikasi Varian D

HASIL KAJIAN

SET PETUA

Berikut merupakan senarai set petua yang telah dihasilkan di dalam kajian yang dijalankan berdasarkan kepada format Snort dengan mengambilkira carta alir pengesanan trafik komunikasi setiap varian.

i. Varian A
- Menghalang dan merekod paket trafik yang cuba untuk mengakses ke laman *trafficconverter.biz* untuk varian A

drop tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"Conficker A - trafik ke trafficconverter.biz dikesan"; flow:to_server,established; content:"Host: trafficconverter.biz"; nocase; sid:1000001;)

- Menghalang dan merekod paket trafik yang cuba untuk mengakses ke Titik Pertemuan untuk varian A
drop tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"Conficker A - Hubungan ke Titik Pertemuan dikesan"; flow:to_server,established; content:"/search?q="; http_uri; pcre:"/\/search\?q=\d+&aq=7/"; sid:1000002;)

ii. Varian B, C dan E
- Menghalang dan merekod paket trafik yang cuba untuk mengakses ke Titik Pertemuan untuk varian B,C dan E

drop tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"Cecacing Conficker B, C atau E – Hubungan ke Titik Pertemuan dikesan "; flow:to_server,established; content:"/search?q="; http_uri; pcre:"/\/search\?q\=\d+/"; sid:100003;)

iii. Varian D
- Menghalang dan merekod paket trafik perangkai padanan varian D untuk kedua-dua arah (inbound dan outbound)

drop udp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:" Trafik perangkai padanan Conficker D - outbound "; flow:to_server; dsize:>19; byte_test:1, &, 1, 17; sid:100004;)
drop udp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:" Trafik perangkai padanan Conficker D – inbound "; flow:to_client; dsize:>19; byte_test:1, &, 1, 17; sid:100005;)

dsize:>19 - saiz data paling kecil UDP Ping yang berkaitan adalah 20 bytes
byte_test:1, &, 1, 17 – semakan terhadap nilai bait ke 18 (kedudukan bait dikira dari 0) dan dibanding nilai 1 (00000001). Dalam semakan byte_test ini, sebarang nilai yang bukan kosong bermaksud ianya memenuhi syarat semakan.

HASIL PENGUJIAN

Tujuan langkah ini dilaksanakan adalah untuk menguji keberkesanan set petua yang dihasilkan dalam menghalang paket trafik cecacing ini daripada memulakan proses komunikasinya dalam memuatturun sebarang binari atau muat beban (sama ada melalui akses Titik Pertemuan atau perangkai padanan atau kedua-duanya). Pengujian ini akan melihat dari sudut kejayaan set petua yang dihasilkan dalam menghalang proses komunikasi seperti yang dinyatakan dalam kajian ini serta jika terdapat berlakunya keadaan positif palsu (*false positive*) dalam pengimplementasian set petua terhadap data trafik setiap varian yang dikaji. Keputusan ujian diperolehi daripada pemerhatian dan perbandingan di antara data trafik ujian dengan data trafik kawalan. Sebanyak 5 sampel data trafik (waktu dan hari yang berbeza tetapi tempoh yang sama) bagi setiap varian telah diuji bagi melihat keberkesanan set petua yang dihasilkan. Jadual 3 hingga Jadual 7 di bawah menunjukkan hasil daripada pengujian yang dilaksanakan terhadap set petua ini.

Jadual 3 Keputusan ujian terhadap Varian A

Sampel	**1**	**2**	**3**	**4**	**5**
Berjaya dihalang	√	√	√	√	√
Positif palsu	x	x	x	x	x

Jadual 4 Keputusan ujian terhadap Varian B

Sampel	**1**	**2**	**3**	**4**	**5**
Berjaya dihalang	√	√	√	√	√
Positif palsu	x	x	x	x	x

Jadual 5 Keputusan ujian terhadap Varian C

Sampel	**1**	**2**	**3**	**4**	**5**
Berjaya dihalang	√	√	√	√	√

Positif palsu	x	x	x	x	x

Jadual 6 Keputusan ujian terhadap Varian D

Sampel	**1**	**2**	**3**	**4**	**5**
Berjaya dihalang	√	√	√	√	√
Positif palsu	√	√	√	√	√

Jadual 7 Keputusan ujian terhadap Varian E

Sampel	**1**	**2**	**3**	**4**	**5**
Berjaya dihalang	√	√	√	√	√
Positif palsu	x	x	x	x	x

PERBINCANGAN

Berdasarkan kepada analisa dan kajian yang dijalankan, didapati bahawa cecacing ini memperolehi sebarang binari atau muat beban daripada penulisnya melalui tiga kaedah iaitu akses ke laman *trafficconverter.biz* (bagi varian A sahaja), akses ke Titik Pertemuan melalui akses kepada nama domain berbeza yang dijana setiap hari (semua varian) dan melalui kaedah akses secara perangkai padanan (bagi varian D). Kajian ini juga mendapati bahawa setiap proses komunikasi akan dimulakan oleh komputer yang telah dijangkiti terlebih dahulu. Oleh yang demikian, dalam menangani ancaman cecacing Conficker ini adalah didapati bahawa dengan menghalang paket trafik pertama yang berkaitan dengan laluan komunikasi cecacing ini daripada dihantar oleh komputer yang dijangkiti daripada berjaya dihantar keluar.

Berdasarkan pemerhatian dan analisa yang dilaksanakan dalam kajian ini juga mendapati bahawa tiada sebarang muatturun binari melalui Titik Pertemuan serta Perangkai Padanan oleh Komputer Ujian. Walaubagaimanapun, terdapat beberapa balasan daripada Titik Pertemuan yang boleh mendedahkan komputer yang dijangkiti serta organisasi umumnya terhadap ancaman keselamatan akibat daripada penetapan session ID dalam cookie (*Session Fixation*) serta pelencongan trafik ke beberapa buah laman web yang dikenalpasti sebagai laman web hasad. Selain itu, fungsi pertahanan kendiri Conficker iaitu dengan melumpuhkan semua fungsi pertahanan keselamatan komputer yang dijangkiti boleh mendedahkan aset maklumat dalam organisasi kepada ancaman keselamatan yang lebih serius. Kajian yang dijalankan juga mendapati bahawa matlamat penulis semua varian Conficker adalah untuk memastikan semua mesin yang telah dijangkiti olehnya sentiasa berada di dalam kawalannya serta menjadikannya hak milik mereka sepenuhnya.

Walaubagaimanapun, berdasarkan hasil pengujian terhadap set petua yang dibangunkan dalam kajian ini mendapati bahawa ianya berjaya menghalang komputer yang dijangkiti daripada memulakan proses komunikasi dalam memuatturun sebarang binari atau muat beban daripada penulisnya. Meskipun terdapat peratusan kecil berlakunya positif palsu terhadap set petua yang dihasilkan untuk perangkai padanan bagi varian D, setelah diselidik ianya berpunca daripada penggunaan perisian komunikasi multimedia secara rangkaian iaitu perisian Skype. Namun demikian, positif palsu dalam kes ini boleh diabaikan kerana penggunaan perisian panggilan video seperti ini adalah dilarang kecuali dalam kes-kes khas yang tertentu oleh organisasi terutamanya jabatan kerajaan. Walaubagaimanapun, jika terdapat keperluan untuk menggunakan perkhidmatan komunikasi multimedia berasaskan rangkaian ini, penambahan nombor port berkaitan ke dalam set petua yang dihasilkan dengan menggunakan format !nombor port boleh dilaksanakan dengan mudah tanpa mengganggu fungsi utama set petua tersebut (Contoh : !5060 untuk Session Initiation Protocol (SIP)).

KESIMPULAN

Kajian ini telah mengkaji berkaitan dengan ancaman cecacing Conficker terutamanya dari segi bagaimana ianya berfungsi di dalam persekitaran rangkaian melalui kajian dan analisis terhadap sampel serta data trafik yang dijana oleh komputer yang telah dijangkiti olehnya. Melaluinya, rangka kerja setiap varian serta ciri-ciri unik setiap varian telah dikenalpasti. Seterusnya carta alir dalam melaksanakan semakan terhadap setiap paket trafik rangkaian bagi mengesan kehadiran trafik yang berkaitan dengan mekanisma komunikasi Conficker turut dihasilkan di dalam kertas kajian ini. Carta alir ini dapat membantu dalam penghasilan set petua sistem pengesanan dan pencegahan pencerobohan berasaskan rangkaian Snort dalam kajian ini. Carta alir yang dihasilkan juga boleh digunakan oleh sistem pengesanan dan pencegahan pencerobohan yang lain dalam membangunkan set petua atau set peraturan dalam menangani ancaman Conficker ini.

Berdasarkan kepada hasil pengujian yang dijalankan terhadap set petua yang dihasilkan dalam kajian ini, didapati bahawa set petua yang dibangunkan berjaya menghalang komputer yang dijangkiti daripada memulakan proses komunikasi dalam memuatturun sebarang binari atau muat beban. Walaupun terdapat

peratusan kecil terhadap berlakunya positif palsu terhadap set petua untuk perangkai padanan bagi varian D, ianya masih boleh dielakkan dengan melaksanakan perubahan kecil terhadap senarai port yang dikecualikan berdasarkan kepada perisian yang digunakan dalam sesebuah organisasi.

Walaubagaimanapun, sepertimana yang dinyatakan pada awal kajian, penghasilan set petua ini bukanlah bermaksud untuk menghalang sebarang proses jangkitan Conficker dalam rangkaian organisasi. Tujuan set petua yang dibangunkan dalam kajian ini hanyalah menumpukan terhadap menghalang daripada proses komunikasi di antara Komputer Mangsa dengan penulis Conficker dalam menerima atau menghantar sebarang muat beban atau binari yang berkaitan. Seterusnya untuk menghalang impak kerosakan yang lebih besar kepada aset maklumat organisasi.

CADANGAN KAJIAN LANJUTAN

Beberapa cadangan kajian masa hadapan telah dikenal pasti agar kajian ini dapat dikembangkan dan ditingkatkan lagi. Oleh itu, cadangan-cadangan tersebut adalah seperti berikut:-

i. Mengkaji kaedah pertahanan lain yang boleh menghalang ancaman Conficker;
ii. Mengkaji dengan lebih mendalam sejauh mana impak Conficker terhadap keselamatan maklumat organisasi;
iii. Mengkaji faktor-faktor yang mempengaruhi tahap keaktifan Conficker yang semakin meningkat walaupun setelah hampir 7 tahun kewujudannya dikesan kali pertama;
iv. Membangunkan rangka kerja asas bagi pelaksanaan analisis perisian hasad dan penghasilan set petua untuk sistem pengesanan pencerobohan.

PENUTUP

Secara keseluruhannya, kajian ini telah berjaya mengenalpasti titik komunikasi penting seterusnya menghasilkan set petua untuk kegunaan sistem pengesanan dan pencegahan pencerobohan berasaskan rangkaian Snort dalam menangani ancaman cecacing Conficker . Kajian ini juga menghasilkan rangka kerja setiap varian Conficker dalam persekitaran rangkaian serta carta alir semakan pengesanan trafik Conficker dalam persekitaran rangkaian. Berdasarkan kepada penghasilan yang dihasilkan, maka kajian ini diharapkan boleh dijadikan asas rujukan dalam melaksanakan kajian lain terhadap cecacing Conficker ini selain menggunakan metodologi kajian ini dalam melaksanakan kajian berkaitan dengan menangani ancaman perisian hasad atau cecacing lain yang mempunyai ciri-ciri yang hampir sama. Ianya boleh membantu pentadbir rangkaian dalam menghalang daripada berlaku kebocoran maklumat kepada pihak yang tidak sepatutnya seterusnya memelihara aset organisasi.

RUJUKAN

[1] Cisco, “Cisco Global Cloud Index : Forecast and Methodology , 2013 – 2018,” 2013.
[2] F. Gens, “Worldwide and Regional Public IT Cloud Services 2014–2018 Forecast,” 2014.
[3] PEMANDU, *Chapter 12 - Bussiness Services (Driving High-Income Growth Through Business Services)*. 2010.
[4] ITIL, *The Official Introduction to the ITIL Service Lifecycle*. 2007.
[5] L. F. da Silva and F. Brito e Abreu, “An IT Infrastructure Patterns Approach to Improve IT Service Management Quality,” *2010 Seventh Int. Conf. Qual. Inf. Commun. Technol.*, pp. 171–176, Sep. 2010.
[6] P. Mell and T. Grance, “The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology,” 2011.
[7] Q. F. Hassan, “Demystifying Cloud Computing,” *CrossTalk - J. Def. Softw. Eng.*, no. January/February, 2011.
[8] Cisco, “Cisco 2015 Annual Security Report,” *Cisco Inc*, pp. 1–53, 2015.
[9] M. Sikorski and A. Honig, *Practical Malware Analysis*. William Pollock, 2012.
[10] F-Secure, “F-Secure H1 2014 Threat Report,” 2014.
[11] F-Secure, “F-Secure H2 2013 Threat Report,” 2013.
[12] F-Secure, “F-Secure H1 2013 Threat Report,” 2013.
[13] F-Secure, “F-Secure H2 2012 Threat Report,” 2012.
[14] F-Secure, “F-Secure H1 2012 Threat Report,” 2012.
[15] F-Secure, “F-Secure H2 2014 Threat Report,” 2014.
[16] S. Baharom, “Ancaman malware kian membimbangkan,” *Utusan Malaysia*, 2015.
[17] C. M. Guitierrez, W. Jeffrey, and C. M. Furlani, “FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems,” *Nist*, no. FIPS PUB 200, 2006.
[18] S. Kramer and J. C. Bradfield, “A general definition of malware,” *J. Comput. Virol.*, vol. 6, no. 2, pp. 105–114, 2010.

[19] B. J. Laxmi, J. S. Reddy, and K. Kirthikumar, "A Behavioral Characterization of Proximity Malware Detection Approach Which Based on Bayesian Model," *Int. J. Mag. Eng. Manag. Res.*, vol. 2, no. April, pp. 11–15, 2015.

[20] Kaspersky Lab, "Types of Malware - Malware Classification," *Internet Security Centre*, 2012. [Online]. Available: http://www.kaspersky.com/internet-security-center/threats/malware-classifications. [Accessed: 10-Jun-2015].

[21] W.-J. Tsaur, Y.-C. Chen, and B.-Y. Tsai, "A New Windows Driver-Hidden Rootkit Based on Direct Kernel Object Manipulation," pp. 679–684, 2009.

[22] J. Bauer, M. Van Eeten, and T. Chattopadhyay, "ITU Study on the Financial Aspects of Network Security: Malware and Spam," *ICT Appl. Cybersecurity Div.*, no. July, 2008.

[23] E. Kovacs, "MiniDuke Malware Used Against European Government Organizations," 2013.

[24] C. Wysopal, C. Eng, and T. Shields, "Static detection of application backdoors," *Datenschutz und Datensicherheit - DuD*, vol. 34, no. 3, pp. 149–155, 2010.

[25] M. S. TechCenter, "Microsoft Security Bulletin MS08-067 - Critical," *Microsoft TechNet*, 2008. [Online]. Available: https://technet.microsoft.com/library/security/ms08-067.

[26] P. Porras, H. Saidi, and V. Yegneswaran, "AN ANALYSIS OF CONFICKER'S LOGIC AND RENDEZVOUS POINT," 2009.

[27] K. Brian, "$72M Scareware Ring Used Conficker Worm," *krebsonsecurity.com*, Jun-2011.

[28] J. Kirk, "Ukraine Disrupts $72M Conficker Hacking Ring," *IDG News Service*, 23-Jun-2011.

[29] D. Bilar, G. Cybenko, and J. Murphy, *Moving Target Defense II: Application of Game Theory and Adversarial Modeling*. Springer Science & Business Media, 2013.

[30] D. Piscitello, "Conficker summary and review," pp. 1–18, 2010.

[31] S. Shin, G. Gu, N. Reddy, and C. P. Lee, "A Large-Scale Empirical Study of Con fi cker," vol. 7, no. 2, pp. 676–690, 2012.

[32] C. Zhang, S. Zhou, and B. M. Chain, "Hybrid spreading of the Internet worm Conficker," *arXiv.org > cs > arXiv1406.6046v3*, no. 1, pp. 1–7, Jun. 2014.

[33] Isaca, "An Introduction to the Business Model for Information Security," *Inf. Secur.*, pp. 1–28, 2009.

[34] Symantec, "W32.Downadup," *Security Response*, 2013. [Online]. Available: http://www.symantec.com/security_response/writeup.jsp?docid=2008-112203-2408-99. [Accessed: 01-Jan-2015].

[35] B. Nahorney, "The Downadup Codex," 2009.

[36] Microsoft, "Virus alert about the Win32/Conficker worm," 2009. [Online]. Available: http://support.microsoft.com/kb/962007.

[37] M. Antonakakis, R. Perdisci, D. Dagon, W. Lee, and N. Feamster, "Building a Dynamic Reputation System for DNS," *Proceeding USENIX Secur. Symp.*, 2010.

[38] H. Tiirmaa-Klaar, J. Gassen, E. Gerhards-Padilla, and P. Martini, *Botnets*. Google Ebook, 2013.

[39] Y. Mehmood, M. A. Shibli, U. Habiba, and R. Masood, "Intrusion Detection System in Cloud Computing: Challenges and opportunities," *2013 2nd Natl. Conf. Inf. Assur.*, pp. 59–66, Dec. 2013.

[40] C. N. Modil, D. R. Patell, A. Patd, and R. Muttukrishnan, "Bayesian Classifier and Snort based Network Intrusion Detection System in Cloud Computing," *IEEE*, no. July, 2012.

[41] C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, and Q. Wu, "AVOIDIT : A Cyber Attack Taxonomy," 2009.

[42] a. a. Waskita, H. Suhartanto, P. D. Persadha, and L. T. Handoko, "A simple statistical analysis approach for Intrusion Detection System," May 2014.

[43] M. Vasilescu, L. Gheorghe, and N. Tapus, "Practical Malware Analysis based on Sandboxing," *RoEduNet Conf. 13th Ed. Netw. Educ. Res. Jt. Event RENAM 8th Conf. 2014*, pp. 1–6, 2014.

[44] H. J. Li, C. W. Tien, C. W. Tien, C. H. Lin, H. M. Lee, and A. B. Jeng, "AOS: An optimized sandbox method used in behavior-based malware detection," *Proc. - Int. Conf. Mach. Learn. Cybern.*, vol. 1, pp. 404–409, 2011.

[45] P. M. Wrench and B. V. W. Irwin, "Towards a Sandbox for the Deobfuscation and Dissection of PHP Malware," *Inf. Secur. South Africa (ISSA), 2014*, no. November, pp. 1 – 8, 2014.

[46] S. Jana, D. E. Porter, and V. Shmatikov, "TxBox: Building secure, efficient sandboxes with system transactions," *Proc. - IEEE Symp. Secur. Priv.*, pp. 329–344, 2011.

[47] H. Qiu and F. C. C. Osorio, "Static malware detection with Segmented Sandboxing," *Proc. 2013 8th Int. Conf. Malicious Unwanted Softw. "The Am. MALWARE 2013*, pp. 132–141, 2013.

[48] M. Christodorescu, S. Jha, S. A. Seshia, D. Song, and R. E. Bryant, "Semantics-Aware Malware Detection," *2005 IEEE Symp. Secur. Priv.*, 2005.

[49] A. Moser, C. Kruegel, and E. Kirda, "Limits of static analysis for malware detection," *Proc. - Annu. Comput. Secur. Appl. Conf. ACSAC*, pp. 421–430, 2007.