ANALISA FITUR PAKET DALAM TEKNIK PENYUSUPAN KELUAR DATA

ROSLINAWATI ABDUL RAHMAN
MOHD ZAMRI MURAH

Fakulti Teknologi dan Sistem Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Data dilihat sebagai satu komoditi kritikal dalam menguasai dunia siber dan dengan pemesatan penggunaan internet, ianya turut menimbulkan isu mengenai keselamatan data. Pencerobohan data adalah satu isu yang memerlukan strategi yang strategik dalam mengurus isu ini dan keperluan bagi mengenalpasti paket berkod hasad adalah satu perkara kritikal dalam mengurus isu ini dengan lebih sistematik. Salah satu teknik dalam serangan siber adalah melalui penyusupan keluar data dan kajian mengenainya terutama sekali melalui protokol HTTP adalah terbatas. Kajian ini menganalisa anomali paket melalui protokol HTTP dengan menggunakan beberapa instrumen penyusupan keluar data untuk lebih memahami fitur paket tersebut. Hasil dapatan ini seterusnya digunakan bagi menulis peraturan bagi mengekang sebarang percubaan perncerobohan.

1. PENDAHULUAN

Internet telah memasuki pasaran Malaysia sejak tahun 1995 dan kini menjadi satu keperluan di kalangan masyarakat pelbagai lapisan umur. Keupayaan mewujudkan sfera awam kepada masyarakat dalam membincangkan sesuatu isu secara maya adalah salah satu kunci yang menzahirkan keperluan ini (Abd Rahman 2006; Dahlgren 2005). Statistik menunjukkan pengguna internet di Malaysia telah berkembang pada 2014 sebanyak 3.1% kepada 6.4 juta langganan dengan kadar penembusan isi rumah mencapai 67.2% pada akhir Jun 2014 berbanding pada akhir Jun 2013 sebanyak 6.2 juta dengan kadar penembusan isi rumah mencapai 66.8% (Ekonomi 2014). Hasil statistik ini mencuraikan perubahan keperluan internet daripada satu komoditi yang dulu dianggap mewah (*luxury good)* kepada komoditi yang menjadi keperluan *(need)* pengguna.

Peranan yang dimainkan oleh media sosial juga telah berubah daripada satu wadah komunikasi kepada agen perubah, agen provokasi dan agen penyampai (Abd Rahman 2006). Laporan Ekonomi 2013/2014 (2014) terbitan Kementerian Kewangan mengindikasikan bahawa pengguna internet di Malaysia telah mencapai 25 juta orang berbanding 18 juta pada 2012, Peningkatan terhadap perkhidmatan jalur lebar ini turut dilaporkan di dalam Laporan Tahunan Program Transformasi Negara 2015 (2016) di Jadual 1.

Copyright@FTSM

Jadual 1 Laporan Peningkatan Keperluan Rakyat Malaysia Terhadap Penggunaan Perkhidmatan Jalur Lebar dan Tanpa Wayar

No	EPP	KPI	Sasaran	Sebenar
1.	EPP7 : Jalur Lebar untuk Semua	Bilangan port yang menyediakan jalur lebar berkelajuan tinggi di kawasan pinggir bandar (SUBB).	55,000	88,588
		Peratusan akses (liputan) jalur lebar berkelajuan tinggi tanpa wayar LTE.	58%	53.5%
		Bilangan port yang menyediakan jalur lebar berkelajuan tinggi dengan kelajuan hingga 100Mbps di ibu negeri dan bandar utama.	76,000	106,854
2.	EPP8 : Memperluaskan langkauan	Jumlah tapak program baru yang telah dikomisyenkan.	950	983
3.	EPP9 : Rangkaian Serantau	Peratusan pelaksanaan bagi pemasangan kabel dasar laut (menghubungkan Sabah, Sarawak dan Semenanjung Malaysia).	45%	35%
		Peratusan penyiapan pelaksanaan kabel dasar laut antarabangsa.	50%	50%

Sumber: (Unit Perancang Ekonomi 2016)

Statistik ini secara tidak langsung menggambarkan keperluan jalur lebar dalam kehidupan seharian rakyat Malaysia. Peningkatan penggunaan jalur lebar yang sangat ketara bagi tahun 2016 berbanding sasaran yang ditetapkan menunjukkan keperluan yang semakin meningkat di dalam penggunaan internet dari skop penggunaan di Malaysia.Kajian ini mencadangkan satu model perkongsian sumber data dan skema pangkalan data SPR di antara agensi-agensi yang terlibat untuk penghantaran dan pertukaran data yang lengkap dan terkini melalui konsep teknologi perkhidmatan web.

1.1 Serangan Siber

Peningkatan di dalam penggunaan internet menghasilkan kesan domino terhadap serangan siber menjadikan ia satu realiti yang perlu diurus secara strategik dan berkesan sepanjang masa (Bruce Schneier 2010). Para penyelidik meramalkan bahawa komunikasi perisian hasad di masa hadapan akan menjadi lebih sukar untuk dikesan dan akan berevolusi dengan mengadaptasikan diri dengan kaedah serta pendekatan keselamatan yang diamalkan menjadikan ianya lebih sukar untuk diurus (Hermans 2013; Kotulic & Clark 2004; Wendzel 2014). Kajian lalu mengesan sebanyak 62% responden bersedia untuk melibatkan diri dengan melakukan serangan siber samada secara atas talian atau luar talian (Holt 2012). Beberapa kajian lain turut mengaitkan kepelbagaian tingkah laku godaman adalah berkaitan dengan tahap kemahiran teknikal yang berbeza (Bossler & Burrus 2011; Holt 2007). Statistik ini jelas menzahirkan kewujudan ancaman serangan siber dan turut disokong dengan kenyataan oleh Prof. John Arquilla, pakar penganalisa hubungan antarabangsa (Geers et al. 2015).

Serangan siber yang melibatkan kelangsungan hidup adalah disokong dengan sejarah yang telah berlaku. Serangan perisian hasad terhadap sektor kewangan Korea Selatan pada 2013 yang mengakibatkan kelumpuhan jaringan kepada 48,000 komputer peribadi dan

Copyright@FTSM

pelayan dan menjejaskan sektor perniagaan dan juga sektor penyiaran (Choe Sang-Hun 2013). Perisian hasad juga adalah penyebab institusi kewangan Bangladesh digegarkan pada 4 February, 2016 yang menyebabkan kerugian sebanyak USD 81 juta (Reuters 2016). Sektor pembekalan kuasa juga tidak terkecuali, mengambil contoh satu serangan terancang dilakukan pada tahun 2015 secara serentak terhadap tiga syarikat pembekalan kuasa Ukraine – Kyivoblenergo, Prykarpattyaoblenergo and Chernivtsioblenergo mengakibatkan 225,000 pelanggan tidak mempunyai sumber perbekalan kuasa (E-Isac 2016; FireEye Industry Inc 2016) manakala kes Banner Health di Amerika Syarikat yang menjejaskan 3.7 juta individu apabila maklumat kritikal dan sensitif digodam (Laventhal 2016) menunjukkan tiada batasan sektor di dalam serangan siber ini. Malaysia juga tidak terkecuali dalam isu serangan siber ini melalui sesi Perbincangan Meja Bulat yang diadakan di Universiti Kebangsaan Malaysia (UKM) bersama Cyber Security pada 2016 turut memaklumkan penyenaraian Malaysia sebagai negara ke enam dengan kadar 13.65% penggunanya digodam.

Serangan terhadap infrastruktur elektronik yang menyokong infrastruktur kritikal seperti sumber kuasa dan kewangan mampu mewujudkan panik dalam skala yang besar (*mass panic*) (Brenner 2009; Holt & Schell 2011). Kaitan yang rapat antara ekonomi dan kehidupan seharian menjadi platform yang kukuh menyokong kesetaraan serangan siber terhadap infrastruktur kritikal dengan serangan keganasan fizikal (Holt 2013) dan dalam kata lain, sebarang serangan ke atas infrastruktur kritikal secara maya mempunyai impak yang memberi kesan langsung seperti mana impak serangan di dunia sebenar dan juga terhadap kelangsungan hidup (Denning 2011; Kilger 2011; Marjie T. Britz 2010).

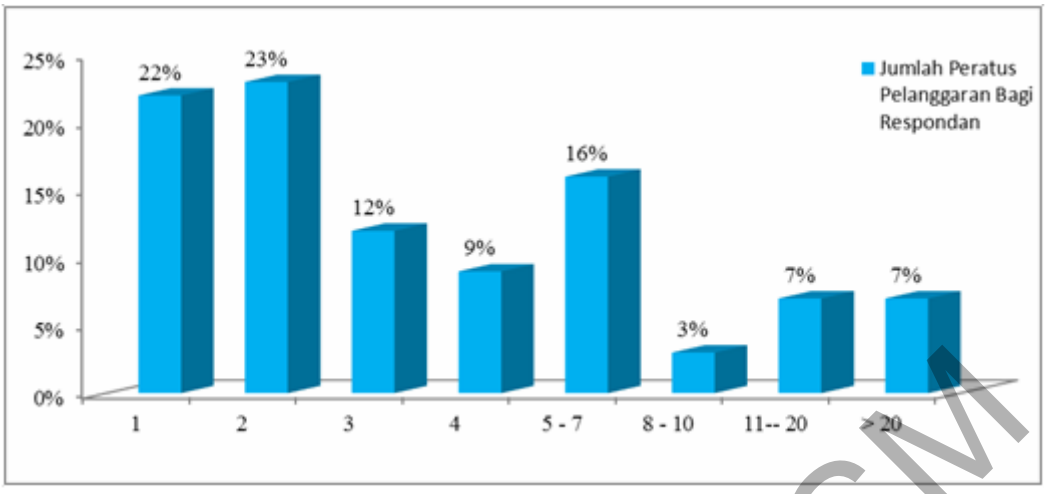
Ini merumuskan bahawa organisasi perlu mengurus ancaman siber dengan lebih holistik dan teratur kerana sebarang ancaman siber yang berskala besar mampu memberikan impak negatif terhadap kelangsungan hidup orang awam.

1.2 Penyusupan Keluar Data

Elemen kritikal dalam pengaplikasian strategi perlindungan maklumat yang holistik adalah melalui aktiviti pengesanan (*detect*) serta pengurangan (*mitigate*) (Berk, Giani & Cybenko 2005; Miranda 2011; Rashid et al. 2013; Villeneuve & Bennett 2012). Pengaplikasian taktik yang berkesan dalam mengesan ancaman serangan mampu mengurangkan kerugian kehilangan maklumat kritikal dan sensitif yang ditanggung oleh organisasi serta berpotensi dalam melindungi organisasi daripada serangan di masa hadapan.

Pencerobohan keselamatan melalui serangan siber wujud dalam pelbagai bentuk dan salah satu teknik serangan siber adalah penyusupan keluar data dan ia menjadi satu mekanisme serangan yang acapkali dikaitkan dengan serangan siber (Fallis 2013; Information Is Beautiful.Net 2017). Verizon mengesan bahawa enam (6) insiden pencerobohan data berlaku bagi satu respondan dan ini dizahirkan melalui Rajah 1.2 (Verizon 2016). Berdasarkan statistik, penyusupan keluar data adalah satu realiti yang perlu diurus dengan lebih sistematik.

Copyright@FTSM



Rajah 1.2 Kajian Mengenai Kekerapan Pelanggaran Keselamatan Data

Laporan pelanggaran yang dikesan dari Intel Security (2014) menunjukkan bahawa trend terhadap pencerobohan data sensitif adalah satu trend yang semakin meningkat dan antara organisasi besar yang turut diserang melalui teknik penyusupan keluar data adalah seperti Yahoo dan juga Monsack Fonseca (Cody 2015; Information Is Beautiful.Net 2017) .

Penggodam yang berjaya menceroboh rangkaian serta mewujudkan satu kawalan yang berterusan mampu memindahkan maklumat kritikal dan sensitif milik organisasi dengan mudah. Pada peringkat ini adalah sukar bagi pentadbir sistem untuk mengesan sebarang aktiviti khianat dalam rangkaian maklumat sensitif yang diperolehi ini mampu memberi impak yang negatif kepada organisasi terlibat.

Dalam erti kata lain, strategi mengesan aktiviti penyusupan keluar data adalah langkah permulaan bagi mengekang aktiviti tersebut.

1.3 Pernyataan Masalah

Terdapat banyak pandangan yang bersetuju bahawa mekanisme yang menjadi medium dalam penyusupan keluar data adalah pelbagai antaranya pintu belakang *(backdoor)*, protokol pindah fail (*file protocol transfer*, FTP), aplikasi web dan instrument pengurusan Windows *(Windows Management Instrumentation)* (WMI) (Berk et al. 2005; Cody 2015; Fallis 2013; Giani, Berk & Cybenko 2006). Kajian terdahulu turut membuktikan aktiviti godaman penyusupan keluar data wujud dan ia disokong dengan data organisasi yang terlibat antaranya Yahoo (Dan Munro 2015; Dlamini, Eloff & Eloff 2009; Information Is Beautiful.Net 2017; Verizon 2016). Permasalahan menjadi lebih kritikal apabila IT personel yang bertanggungjawab menjaga keselamatan tidak kompeten serta tidak mahir dalam mengenalpasti paket yang mempunyai kod hasad (Hermans 2013; Mancuso et al. 2014; Potter 2011). Imej organisasi yang tercalar dan kerugian yang besar akibat manipulasi data kritikal yang disusup keluar adalah antara impak yang wujud akibat serangan ini.

Kebanyakan kajian terdahulu adalah tertumpu kepada kaedah penyusupan masuk penggodam ke dalam rangkaian (Berk et al. 2005; Born 2010; Choi et al. 2008; CISCO 2015; Koeppen 2014) atau kaedah penggodam melepasi pertahanan keselamatan (Dambala Inc

Copyright@FTSM

2013; Fawcett 2010; Giani et al. 2006; Neal Harris 2013; Payer 2014; Rashid et al. 2013; Seals 2017; V Jyothsna, V V Rama Prasad & Munivara K Prasad 2013; Villeneuve & Bennett 2012) manakala kajian dalam mengenali dalam paket bagi kaedah penyusupan keluar data masih terbatas.

Ini seterusnya mewujudkan permasalahan utama yang membawa kepada kajian ini iaitu mengenali fitur dalam paket khusus kepada protokol HTTP bagi teknik penyusupan keluar data.

Oleh yang demikian, kajian ini bertujuan bagi mengenalpasti fitur dalam paket yang mengandungi kod hasad bagi teknik penyusupan keluar data dan seterusnya menghasilkan peraturan (*rules)* bagi mencegah penyusupan keluar data.

2. LIPUTAN KESUSATERAAN

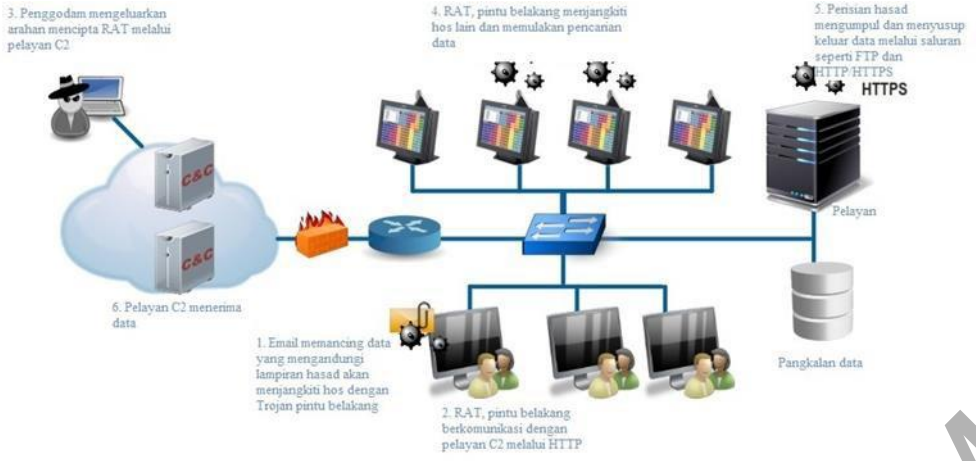
2.1 Latar Belakang

Jenayah siber telah banyak berevolusi sama ada dari segi motif dan juga peningkatan dari segi kecanggihan. Aktiviti godaman yang dilakukan oleh kumpulan penggodam seperti Lulzsec dan juga Anonymous lebih bermotifkan penjenamaan dan propaganda yang menyebabkan gangguan sistem, sebaran maklumat sulit dan juga *web defacement* (Rashid et al. 2013; Wahab 2016). Ramai penyelidik sependapat bahawa ancaman dalam aktiviti godaman adalah satu jenayah terancang bermotifkan pengintipan maklumat industri dari pesaing dan juga pengintipan siber dari aktor negara (Brenner 2009; Denning 2011; Holt & Schell 2011; Laventhal 2016; Marjie T. Britz 2010) manakala kecanggihan teknologi godaman juga dilihat dari kes-kes seperti serangan Stuxnet, Flame dan Duqu (InfoSec Institute 2015; Zetter 2014). Kajian oleh Intel Security (2015) mengenai pencerobohan data ke atas organisasi dengan 522 respondan mengesan 6 insiden berlaku bagi setiap respondan. Ini secara harafiah menzahirkan tahap kritikal keselamatan siber di dalam organisasi.

2.2 Teknik Penyusupan Keluar Data

Senario tipikal bagi penyusupan keluar data adalah mewujudkan jalinan perintah dan kawal (*command and control)* (C2) antara penggodam dan sasaran, bertujuan untuk mengawal peranti mangsa dari jauh (Cody 2015; Fallis 2013; Rashid et al. 2013).

Copyright@FTSM



Rajah 2 Gambaran Visual Teknik Penyusupan Keluar Data

Sumber : (Rashid et al. 2013)

Penggodam akan menyusup masuk ke dalam komputer hos seterusnya mengeksploitasi semua elemen kelemahan keselamatan yang wujud dalam organisasi. Contoh yang seringkali terjadi ialah apabila kakitangan dalaman organisasi membuka email memancing data yang mengandungi lampiran hasad seperti CVE-2012-0158, seterusnya menjangkiti komputer hos dengan virus yang kemudiannya mencipta instrumen akses jauh (*remote access tools)* (RAT) atau pintu belakang *(back door)* bagi memberi C2 kepada penggodam dalam mencapai objektif mutakhir mereka (Cody 2015; Fallis 2013; Fraga, Banković & Moya 2012; Goode 2010).

2.3 Kajian Terdahulu : Penyusupan Keluar Data / *Data Exfiltration*

Kajian terdahulu bagi mengenalpasti penggodam telah merumuskan pelaku kepada tiga kategori iaitu Aktor Negara, Kumpulan Jenayah Terancang dan aktivitis godaman atau hacktivis serta mempunyai motivasi yang tertentu dalam melakukan godaman seperti risikan, pengaruh, kewangan, reputasi dan sosial dizahirkan seperti Rajah 2 (Cody 2015; Guri et al. 2016; Lough 2001; Obszyński 2015). Ini disokong dengan laporan McAfee (2015) yang mengesan peratus pelaku di dalam godaman secara penyusupan keluar data di mana penggodam dari luar sebanyak 57 peratus manakala penggodam dari dalam organisasi pula terbahagi kepada dua kategori iaitu dengan niat sebanyak 22 peratus dan tanpa niat sebanyak 21 peratus.

Copyright@FTSM

Rajah 2.3.1 Klasifikasi dan Motif Godaman Yang Dizahirkan Melalui Kajian Lepas
Sumber : (Cody 2015; Guri et al. 2016; Lough 2001; Obszyński 2015)

Rajah 2.3.2 Komponen Utama Dalam Merealisasikan Penyusupan Keluar Data
Sumber : (Cody 2015)

Antwerp (2011) melalui kajian beliau menjelaskan lagi bahawa penyusupan keluar data mempunyai komponen utama iaitu penggodam, data yang disasarkan, manipulasi data, pemindahan data dan infrastruktur bagi merealisasikan penyusupan keluar data dan ini di sokong dengan kajian lanjutan yang dilaksanakan oleh Cody (2015).

Miranda (2011) di dalam kajiannya mengulas mengenai fasa yang wujud di dalam penyusupan keluar data iaitu pengumpulan maklumat, kemasan (*packaging)* dan seterusnya penyusupan keluar data yang diperlukan. Beliau seterusnya berpandangan fasa yang diperincikan adalah satu fasa umum untuk mana-mana aktiviti penyusupan keluar data.
Antwerp (2011) di dalam kajiannya turut mengklasifikasikan metodologi penyusupan keluar data berdasarkan jalur lebar (*bandwith)* dan tahap tersembunyi (*covert)* dan menghasilkan analisa seperti Jadual 2 di bawah:

Copyright@FTSM

Jadual 2 Taksonomi Bagi Teknik Penyusupan Keluar Data Yang Dibangunkan Oleh Antwerp Berdasarkan Kepada Bandwith Dan Tahap Tersembunyi

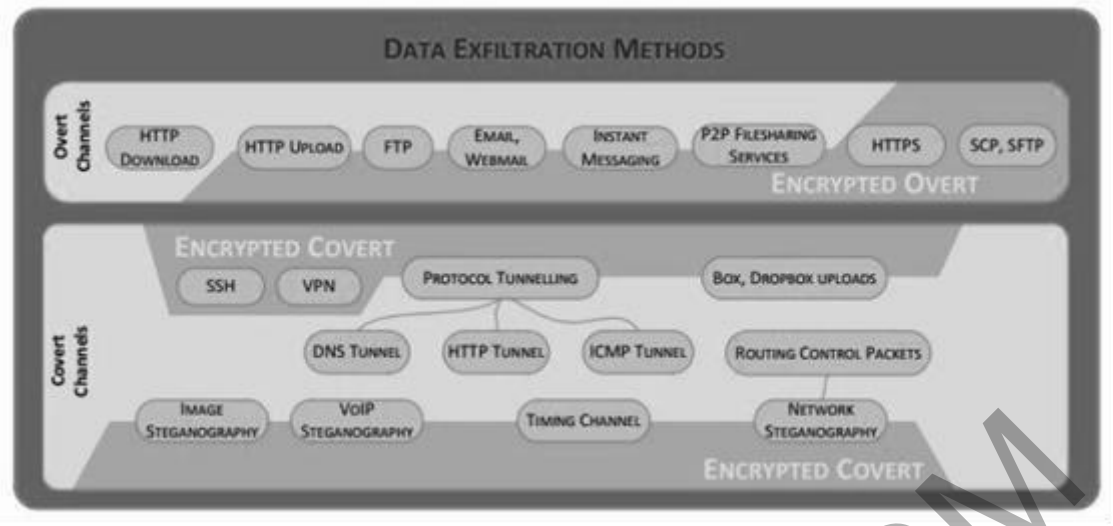
Nama	**Protokol**	**Enkripsi**	***Bandwith***	**Tahap Tersembunyi**
File Transfer	FTP	Ya	5	3
Secure Copy	RCP/SSH	Sentiasa	5	2
HTTP POST	HTTP	Tidak	5	4
SSL HTTP	HTTPS	Sentiasa	5	5
Email	SMTP	Tidak	5	4
SSH Tunnel	SSH	Sentiasa	5	2
Instant Message	IRC/XMPP	Ya	3	4
Echo-Request	ICMP	Tidak	2	4
DNS Tunnel	DNS	Tidak	1	2
Update Comm	HTTP?SOAP	Tidak	5	3
P2P	TCP	Tidak	5	2
Custom IP	IP	Tidak	3	4
Custom TCP	TCP	Tidak	5	3
Custom UDP	UDP	Tidak	4	2

Sumber : (Antwerp 2011)

Kajian yang dilaksanakan oleh Helouet (2005) mengesan penyusupan keluar data berhubung rapat mengenai identifikasi saluran rahsia dan kajian ini seterusnya diperincikan Born (2010). Perbezaan ketara antara kedua pengkaji berkaitan objektif kajian di mana Helouet mengkaji sumber kongsi (*shared resource)* yang berpotensi untuk dimanipulasi sebagai saluran rahsia manakala Born mengkaji penyusupan keluar data berasaskan pelayar melalui saluran rahsia. Ruhiu (2013) pula menyenaraikan tiga perkara kritikal yang perlu ditambahbaik bagi meningkatkan keupayaan keselamatan iaitu fokus kepada pemulihan pasca penyusupan keluar data, pendekatan terhadap polisi jangka pendek dan pendekatan keselamatan yang berkonsepkan ―Perlindungan Maklumat‖ yang lebih holistik dengan penekanan terhadap konsep mengesan dan mengekang penyusupan keluar data.

Kaedah penyusupan keluar data dikesan mampu dilaksanakan melalui dua kaedah utama iaitu sama ada melalui saluran rahsia (*covert channel*) atau saluran sahih (*overt channel*) (Antwerp 2011). Fallis (2013) dan Ruhiu (2013) seterusnya memperincikan dengan lebih jelas dengan mengidentifikasi protokol yang boleh digunakan bagi setiap saluran. Senarai protokol bagi saluran sahih adalah muat turun HTTP, muat naik HTTP, FTP, email dan webmail, pemberitaan instan, perkongsian file bagi servis P2P, HTTPS dan SCP dan SFTP. Manakala bagi saluran rahsia protokol SSH, VPN, terowongan dan Dropbox adalah antara yang boleh diguna pakai.

Copyright©FTSM



Rajah 3 Metodologi Penyusupan Keluar Data

Sumber : (Nduta Dennis Ruhiu 2013)

Hasil kajian tersebut dapat dirumuskan bahawa saluran utama digunakan oleh pengguna sah dalam urusan pemindahan file antara lokasi manakala saluran rahsia (*covert channel)* pula digunakan oleh penggodam bagi mengelakkan dari dikesan melalui pemantauan berasaskan rangkaian dengan cara menyembunyikan data yang diambil (Fallis 2013).

Kajian yang dilaksanakan oleh Awais Rashid (2013) lebih memfokuskan kepada *Advance Persistent Threats* (APT) dan mengesan tiga (3) fasa penyusupan keluar data melalui APT iaitu :

- Fasa 1 melibatkan proses peninjauan (*reconnaissance),* pementasan serangan *(attack staging)* dan jangkitan awal kepada hos (*initial host infection)*
- Fasa 2 melibatkan proses pencerobohan rangkaian (n*etwork intrusion),* kawalan jauh *(remote control),* gerakan rusuk (*lateral Movement),* penemuan data (d*ata discovery),* kegigihan (*persistence)*; dan
- Fasa 3 melibatkan proses pementasan bagi pemilihan pelayan (*staging-server selection),* penyediaan data (*data preparation)* dan penyusupan keluar data (*data exfiltration).*

Kajian yang dilaksanakan oleh Rashid turut mengklasifikasikan data organisasi kepada tiga klasifikasi iaitu peringkat data yang sedang digunakan (*data in use)* , data yang tidak aktif iaitu data yang disimpan secara fizikal di dalam pangkalan data (*data at rest*) serta data yang menyeberangi rangkaian atau disimpan sementara di dalam memori komputer untuk dibaca, dikemaskini dan dikemukakan kepada perkhidmatan pemprosesan data lain *(data in motion)* (Rashid et al. 2013).

Kajian berkaitan protokol HTTP bermula dengan kajian yang dilaksanakan oleh Cabuk (2008) yang mengesan protokol HTTP mampu dimanipulasi sebagai saluran rahsia (*covert channel).* Born (2016) seterusnya membincangkan bahawa protokol HTTP mampu dimanipulasi hanya dengan penggunaan beberapa perisian *(software)* tertentu yang boleh dimanipulasi sebagai instrument dalam penyusupan keluar data.

Copyright@FTSM

2.4 Kesimpulan

Kajian lepas yang dilaksanakan secara jelas menjurus kepada dasar memahami asas pelaku/penggodam, motif dan teknik mengesan godaman secara penyusupan keluar dan juga identifikasi saluran yang digunakan oleh penggodam. Fokus terhadap memahami teknik penyusupan keluar melalui protokol HTTP pula adalah terhad manakala identifikasi dalam mengenalpasti fitur muat beban di dalam paket terlibat tidak diberi penekanan.

Hasil dari jurang kajian terdahulu, maka kajian ini akan lebih menumpukan kepada mengenalpasti fitur muat beban *(payload)* yang mengandungi kod hasad (*malicious code*) di dalam paket melalui protokol HTTP dalam mengidentifikasi paket yang meragukan.

3. METODOLOGI

3.1 REKABENTUK KAJIAN

Memandangkan kajian ini adalah berasaskan kajian eksperimen dan memfokuskan terhadap protokol HTTP maka instrumen yang diguna pakai adalah spesifik kepada pelaksanaan penyusupan keluar data dan dipilih bagi menzahirkan variasi bagi memantau karektor penyusupan keluar data untuk tujuan penganalisaan dan seterusnya sebagai panduan untuk penghasilan peraturan di dalam IPS.

Kajian ini akan dilaksanakan di dalam kondisi yang terkawal di mana satu persekitaran semu dibangunkan sebagai cerminan amalan keselamatan asas yang diamalkan oleh organisasi. Senario yang diaplikasi bagi kajian ini adalah senario pasca eksploitasi iaitu dimana keselamatan komputer mangsa telah berjaya ditembusi dan dikompromi oleh penggodam.

3.2 INSTRUMEN DAN JUSTIFIKASI

Penggunaan instrumen *(tools)* yang bersesuaian amat diperlukan di dalam kajian ini ditambah pula kajian ini mengkhususkan kepada protokol HTTP. Oleh yang demikian bagi melihat persamaan atau perbezaan karektor di dalam muat beban *(payload)* atau muatan sampel paket, instrumen (tools) yang diaplikasi di dalam kajian ini divariasikan bagi memberi kedalaman (*depth*) terhadap analisa yang dilakukan. Pada masa yang sama, setiap instrumen *(tools)* yang dipilih mempunyai fungsi tersendiri dan ini sekaligus memberikan satu pandangan yang lebih jelas terhadap karektor paket yang dianalisa.

Instrumen yang diguna pakai di dalam kajian ini adalah spesifik dengan fungsi-fungsi yang lazim digunakan dalam kaedah penyusupan keluar data seperti fungsi pintasan *(bypass)*, cangkerang songsang (*reverse shell*), cangkerang ikatan (*bind shell*) dan terowongan *(tunneling)*. Instrumen yang digunakan di dalam kajian ini adalah *Fireaway, Badcookie, DET, HTTyHole, Data Exfiltration_HTTP, Firedrill* dan *What2evade*. Penerangan ringkas mengenai fungsi instrumen yang dipakai dizahirkan di dalam Jadual 4.

Copyright@FTSM

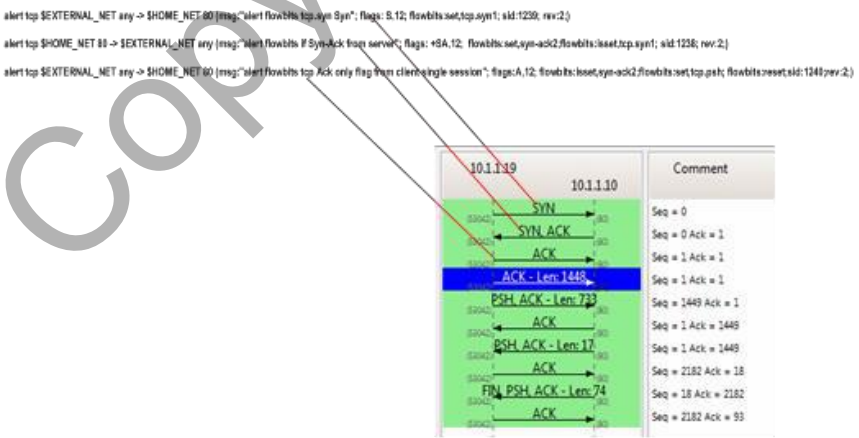
Jadual 3 Fungsi Mengenai Instrumen Yang Diguna Pakai di dalam Kajian Ini

Instrumen	**Fungsi**			
	Pintasan	**Cangkerang Songsang**	**Cangkerang Ikatan**	**Terowongan**
Fireaway	Y		Y	
Badcookie	Y		Y	
DET			Y	
HTTyHOLE	Y	Y		
Data Exfiltration_HTTP	Y	Y		
Firedrill	Y			Y
What2evade	Y			Y

3.3 PENGANALISAAN DAN PENULISAN PERATURAN

Penganalisaan terhadap paket dalam kajian ini menggunakan *Wireshark* bagi memberi penjelasan terhadap fitur paket bagi penyusupan keluar data. Manakala bagi penciptaan tetapan *(rules)*, pengaplikasian ciri (*features)* *Flowbit* di dalam aplikasi *SNORT* digarap sebagai cadangan untuk IPS. Ciri (*feature*) *Flowbit* diadaptasi bagi memberikan korelasi antara tetapan yang ditulis.

Flowbit diguna pakai bagi mewujudkan korelasi antara tetapan dan dizahirkan di dalam Rajah 1 di bawah. Bagi menghuraikan penggunaan *Flowbit* di dalam penulisan peraturan ini, gambaran 10.1.1.19 adalah sasaran manakala 10.1.1.10 adalah pelayan. Untuk sesi normal 3 *way handshake*, peraturan di para pertama ditetapkan dengan nama melalui siri tetapan "flowbits:set,tcp.syn1" manakala bagi peraturan di para kedua dinamakan melalui tetapan "flowbits:set,syn-ack2" dan ditambah dengan tetapan "isset" iaitu "flowbits:isset,tcp.syn1. Tetapan –isset‖ adalah bertujuan mewujudkan korelasi antara tetapan di para pertama dan kedua.



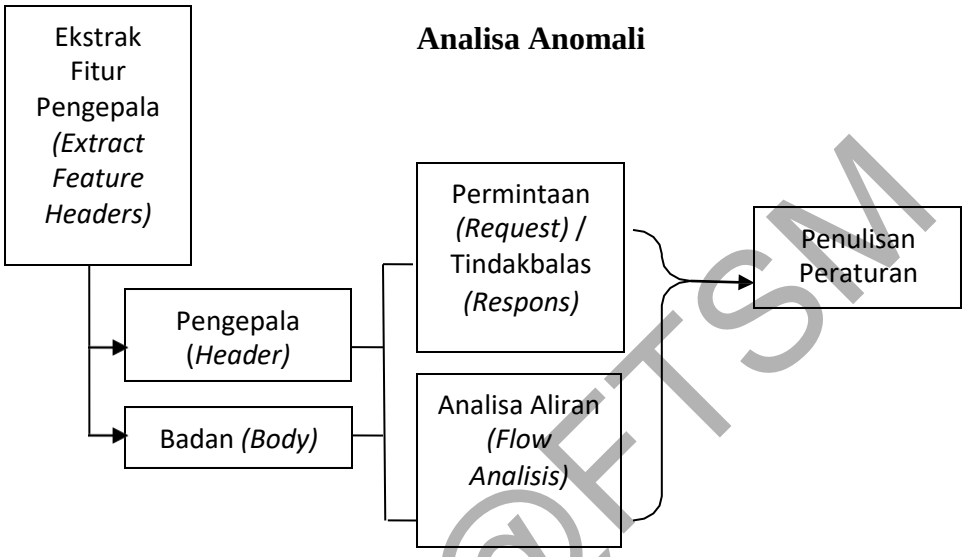
Rajah 1 Contoh Penggunaan Flowbit Di Dalam Menulis Peraturan

Oleh kerana persekitaran yang dibangunkan ini adalah satu persekitaran semu, wujud beberapa kekangan dari segi keperluan keselamatan , peranti serta instrumen yang digunakan dalam merealisasikan kajian ini.

Copyright@FTSM

3.3.1 Simulasi Persekitaran Semu

Simulasi persekitaran semu yang dibangunkan serta aliran kerja kajian digambarkan di dalam Rajah 2 di bawah. Di mana muat beban *(payload)* di dalam paket akan dianalisa melalui dua (2) parameter iaitu permintaan *(request)* / tindakbalas *(response)* dan analisa haluan jabat tangan (*handshake flow analysis*).



Rajah 2 Aliran Kerja Di dalam Persekitaran Semu Yang Dibangunkan

3.3.2 Teknik Kajian

Kod hasad akan disuntik menggunakan kesemua aplikasi *(tools)* yang disenaraikan terdahulu iaitu Fireaway, Badcookie, DET, HTTyHole, Data Exfiltration_HTTP, Firedrill dan What2evade. Seterusnya pengepala (*header)* dan badan *(body)* tersebut diekstrak serta dianalisa berdasarkan dua (2) parameter iaitu permintaan (*request)* serta tindakbalas (*response)* dan haluan jabat tangan *(flow handshake).*

Hasil analisa dari pengepala dan badan paket tersebut membolehkan penulisan peraturan untuk tujuan sekatan dilakukan. Sekiranya paket yang dianalisa tersebut melepasi ―Good List‖ sedia ada dan juga peraturan yang telah ditulis, paket tersebut dibenarkan melalui IPS, sekiranya ianya tidak melepasi piawaian yang ditetapkan, paket tersebut akan digugurkan *(drop).*

3.3.3 Peranti Yang Digunakan

Di dalam melaksanakan kajian ini, peranti dan aplikasi berikut digunakan :

i. Putty;
ii. Komputer riba dengan dua IP address : 192.168.0.20 bagi sasaran dan 192.168.0.200 bagi penggodam;
iii. Virtual Private server (Linux Debian); dan
iv. Node bagi kawalan dan arahan.

Copyright@FTSM

4. HASIL KAJIAN

4.1 Fireaway

Melalui analisa menggunakan *Wireshark*, dikesan wujud fitur muat beban *(payload)* yang kecil pada permulaan data hasil komunikasi antara pengguna dan pelayan. Hasil analisa aliran TCP mengesan kewujudan muat beban untuk penyusupan keluar data dengan jelas melalui Rajah 16 iaitu muat beban yg digunakan tidak mengandungi sebarang identifikasi normal seperti Header HTTP –Host, User-Agent, Accept-Encoding atau kukis.

4.2 Badcookies

Analisa paket mengesan di dalam teknik menggunakan Badcookies, fitur data asal bertukar kepada pengekodan base64 seperti Rajah 18. Data ini dikesan disorok dalam kuki di bahagian pengepala.

4.3 DET

Hasil analisa *Wireshark* mengesan wujud fitur yang tetap apabila mengunakan aplikasi DET HTTP iaitu terdapat muat beban di dalam TCP Flag FIN-ACK . Di dalam kondisi normal, TCP Flag FIN-ACK tidak mempunyai sebarang muat beban. Fitur ini dikesan pada setiap paket yang menggunakan instrument DET.

4.4 HTTyHole

Analisa dari *Wireshark* yang diperolehi dari paket yang menggunakan instrument HTTyHole mengesan satu fitur yang ketara iaitu TCP flags FIN-PSH-ACK dengan muat beban di IPS, fitur ini adalah tidak normal berbanding dengan paket yang biasa digunakan dalam HTTP.

4.5 Data Exfiltration_HTTP

Analisa paket yang dilakukan menggunakan aplikasi *Wireshark* bagi mengesan penyusupan data secara cangkerang songsang (*reverse shell*) mendapati pada TCP FIN-ACK mengandungi kod respon (*response code*) muat beban *(payload) command* –ifconfig‖.

Di dalam keadaan normal TCP FIN-ACK , (samada dari pelayan atau pengguna), TCP FIN-ACK sepatutnya tidak mempunyai muat beban. Ini menunjukkan bahawa ianya adalah satu fitur yang tetap dalam penggunaan Data Exfiltration_HTTP dan hasil ini digunakan sebagai satu langkah pengesanan oleh IPS .

4.6 Firedrill

Berdasarkan penganalisaan pengepala bagi paket menggunakan *Wireshark*, dikesan terdapat abnormaliti di dalam pengepala. Dalam kondisi normal, pada setiap pengepala akan mempunyai parameter pengepala berikut : Host, User-Agent, Accept, Accept-Language dan Accept-Encoding. Hasil paket menggunakan Firedrill mengesan bahawa kesemua parameter pengepala yang dinyatakan tidak terzahir.

Copyright@FTSM

4.7 What2evade

Dalam situasi normal satu sesi yang lengkap bagi transaksi data akan mempunyai elemen berikut : 3 way handshake, sesi data dengan HTP GET/POST request dan 4 way handshake sebagai penutup paket. Keseluruhan elemen ini dipanggil sesi per rentetan (stream).

Mengambilkira sesi per rentetan normal tersebut, analisa menzahirkan sesi data dengan HTP GET/POST request yang berbilang per rentetan (*multiple session per stream*) dalam penggunaan instrument What2evade. Ini jelas menunjukkan abnormaliti paket yang telah dianalisa.

4.8 Rumusan

Satu jadual rumusan anomali hasil kajian yang telah dijalankan menggunakan tujuh (7) instrument penyusupan keluar data dibangunkan melalui Jadual 5 bagi memberikan gambaran menyeluruh pengesanan yang dilaksanakan.

Jadual 4 Rumusan Anomali

Instrumen	**Analisa**		
	Enkripsi	**Kedudukan Pengesanan**	**Catatan**
Fireaway	Tiada	Anomali dikesan pada pengepala	
Badcookie	Enkripsi base64	Dikesan dalam kuki	
DET	Enkripsi tersendiri	Badan (*body*) (*request*)	
HTTyHOLE	Enkripsi tersendiri	Dikesan dalam kuki	
Data Exfiltration_HTTP	Tiada	Badan (*body*) (*response*)	Wujud arahan pada badan (*body*) (*response*)
Firedrill	Enkripsi tersendiri	Pengepala (*Header)*	
What2evade	Enkripsi base64	Badan (*body*) (*request*) Badan (*body*) (*response*)	

Dalam hubungan yang sama, penulisan peraturan bagi mengekang penyusupan keluar data pula bagi kesemua instrumen yang digunakan dirumuskan di dalam Jadual 6 di bawah.

Copyright@FTSM

Jadual 5 Rumusan Penulisan Peraturan

Instrumen	**Penulisan Peraturan**
Fireaway	Mengesan identifikasi normal pada 3 *way handshake*
Badcookie	Mengesan pengekodan base64
DET	Mengesan TCP Flag FIN-ACK dengan muat beban
HTTyHOLE	Mengesan TCP Flag FIN-PSH-ACK
Data Exfiltration_HTTP	Mengesan TCP Flag FIN-ACK yang mengandungi kod respon
Firedrill	Membuat validasi pengepala pelayar (*browser validation*)
What2evade	Mengesan sesi per rentetan yang berbilang

Bagi penulisan peraturan SNORT untuk mengekang penyusupan keluar data ini, ianya dizahirkan mengikut instrument yang digunakan :

4.8.1 Fireaway

Penulisan peraturan Snort untuk mengesan sebarang muat beban yang tidak mempunyai identifikasi normal seperti *Header* HTTP –Host, User-Agent, Accept-Encoding atau kuki dilakukan bagi mencegah kemasukan yang mempunyai fitur tersebut. Dalam hubungan ini, penulisan peraturan Snort adalah seperti di bawah:

#3 handshake flow

alert tcp $EXTERNAL_NET any -> $HOME_NET [80,443] (msg:"alert tcp.syn Syn"; flags: +S,12; flowbits:set,tcp.syn1; flowbits:noalert;sid:55; rev:2;)

alert tcp $HOME_NET [80,443] -> $EXTERNAL_NET any (msg:"alert SynAck from server"; flags: +SA,12; flowbits:isset,tcp.syn1; flowbits:set,syn-ack;flowbits:noalert; sid:56; rev:2;)

alert tcp $EXTERNAL_NET any -> $HOME_NET [80,443] (msg:"alert tcp Ack flags from client"; flags: !SRPUF,12; flowbits:isset,syn-ack;flowbits:set,ACK;flowbits:noalert;flowbits:reset; sid:57; rev:2;)

##

alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"Detect IE browser versi 6 "; flags:+PA,12; pcre:"/(GET|POST|HEAD)/m"; content:"HTTP/1."; content:"Accept"; content:"Host"; nocase; content:"User-Agent:";nocase;content:"Mozilla/"; content:"MSIE"; flowbits:isset,ACK; flowbits:set,IE;flowbits:reset; sid:68; rev:2;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"Detect Mozilla Firefox browser "; flags:+PA,12; pcre:"/(GET|POST|HEAD)/m"; content:"HTTP/1."; content:"Accept"; content:"Host"; nocase; content:"User-

Copyright@FTSM

Agent:";nocase;content:"Mozilla/"; content:"Firefox/"; flowbits:isset,ACK; flowbits:set,MOZILLA;flowbits:reset; sid:69; rev:2;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"Detect Mozilla Firefox browser"; flags:+PA,12; pcre:"/(GET|POST|HEAD)/m"; content:"HTTP/1."; content:"Accept"; content:"Host"; nocase; content:"User-Agent:";nocase;content:"Mozilla/5"; content:"Firefox/"; flowbits:isset,ACK; flowbits:set,Moz;flowbits:reset; sid:70; rev:2;)

##

#drop tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"drop if not Browser IE6 or Firefox winxpi or Firefox "; flags:+PA,12;flowbits:isnotset,IE|MOZILLA|Moz; sid:72;rev:2;)

##

4.8.2 Badcookies

Penulisan peraturan Snort dilakukan bagi mencegah kemasukan yang mempunyai fitur base64 seperti yang dikesan. Sehubungan itu, penulisan *rules* Snort IPS berikut diaplikasi:

#alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg: "Base64 Encoded Data detected" ;base64_decode;base64_data; content:"root:x:0:0:root:/root:/bin/bash" ; sid:600; rev:2;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"Base64 Encoded Data detected"; sid:600;rev:2;)

4.8.3 DET

Pengadaptasian penulisan *rules* Snort dilakukan bagi mencegah kemasukan FIN-ACK yang mempunyai muat beban seperti fitur yang dikesan. Sehubungan itu, penulisan peraturan Snort berikut ditulis seperti berikut:

#3 handshake flow

alert tcp $EXTERNAL_NET any -> $HOME_NET [80,443] (msg:"alert tcp.syn Syn"; flags: +S,12; flowbits:set,tcp.syn1; flowbits:noalert;sid:455; rev:2;)

alert tcp $HOME_NET [80,443] -> $EXTERNAL_NET any (msg:"alert Syn-Ack from server"; flags: +SA,12; flowbits:isset,tcp.syn1; flowbits:set,syn-ack;flowbits:noalert; sid:456; rev:2;)

alert tcp $EXTERNAL_NET any -> $HOME_NET [80,443] (msg:"alert tcp Ack flags from client"; flags: !SRPUF,12; flowbits:isset,syn-ack;flowbits:set,ACK;flowbits:noalert;flowbits:reset; sid:457; rev:2;)

##

Copyright@FTSM

##detect flow from HTTP with GET/POST

alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"HTTP client flowA DET "; flags:+PA,12; pcre:"/(GET|POST|HEAD)/m"; content:"HTTP/1."; content:"Accept"; content:"Host"; nocase; content:"User-Agent:";nocase; flowbits:isset,ACK; flowbits:set,flowA; sid:1988; rev:2;)

alert tcp $HOME_NET 80 -> $EXTERNAL_NET any (msg:"response flowA DET"; content:"HTTP/1"; content:"200 OK" ; flowbits:isset,flowA;flowbits:set,flowB;flowbits:reset;sid:181;rev:2;)

drop tcp $HOME_NET 80 -> $EXTERNAL_NET any (msg:"drop response DET FIN-PSH-ACK"; flags: +FPA; dsize:>1;flowbits:isset,flowB; sid:900;rev:2;)

##

4.8.4 HTTyHole

Usai hasil dapatan tersebut penulisan peraturan Snort yang direka adalah :

alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"alert detect SYN ";flags:+S,12;dsize:<1;flow:to_server,not_established;flowbits:set,1;flowbits:noalert;sid:223;rev:2;)

drop tcp $HOME_NET 80 -> $EXTERNAL_NET any (msg:"drop detect FIN-PSH-ACK";flags:+FPA,12;dsize:>1; flowbits:isset, 1; flowbits:reset; sid:225; rev:2)

4.8.5 Data Exfiltration

Penulisan peraturan Snort perlu ditulis untuk mengesan sebarang FIN-ACK yang mempunyai muat beban dan ianya ditulis seperti di bawah :

alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"alert detect SYN";flags:+S,12; dsize:<1;flow:to_server,not_established;flowbits:set,1; flowbits:noalert;sid:200;rev:2;)

drop tcp $HOME_NET 80 -> $EXTERNAL_NET any (msg:"drop detect FIN-ACK";flags:+FA,12;dsize:>1;flowbits:isset,1;flowbits:reset; sid:201; rev:2)

4.8.6 Firedrill

Bagi menulis peraturan Snort, penambahan peraturan untuk mengesan abnormaliti pada pengepala HTTP perlu dizahirkan. Penzahiran ini dapat ditulis dengan mengadaptasikan pendekatan peraturan pengesahan pelayar HTTP (HTTP *browser validation)* seperti yang digunakan dalam penulisan peraturan mengesan Fireaway di 4.1.1 untuk tujuan pengguguran (*drop*). Dalam hubungan ini, penulisan peraturan Snort adalah seperti berikut :

Validasi Header browser (*Header browser validation*) :

#3 handshake flow

Copyright@FTSM

alert tcp $EXTERNAL_NET any -> $HOME_NET [80,443] (msg:"alert tcp.syn Syn"; flags: +S,12; flowbits:set,tcp.syn1; flowbits:noalert;sid:55; rev:2;)

alert tcp $HOME_NET [80,443] -> $EXTERNAL_NET any (msg:"alert Syn-Ack from server"; flags: +SA,12; flowbits:isset,tcp.syn1; flowbits:set,syn-ack;flowbits:noalert; sid:56; rev:2;)

alert tcp $EXTERNAL_NET any -> $HOME_NET [80,443] (msg:"alert tcp Ack flags from client"; flags: !SRPUF,12; flowbits:isset,syn-ack;flowbits:set,ACK;flowbits:noalert;flowbits:reset; sid:57; rev:2;)

##

alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"Detect IE browser versi 6 "; flags:+PA,12; pcre:"/(GET|POST|HEAD)/m"; content:"HTTP/1."; content:"Accept"; content:"Host"; nocase; content:"UserAgent:";nocase;content:"Mozilla/";content:"MSIE";flowbits:isset,ACK; flowbits:set,IE;flowbits:reset; sid:68; rev:2;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"Detect Mozilla Firefox browser "; flags:+PA,12; pcre:"/(GET|POST|HEAD)/m"; content:"HTTP/1."; content:"Accept"; content:"Host"; nocase; content:"User-Agent:";nocase;content:"Mozilla/"; content:"Firefox/"; flowbits:isset,ACK; flowbits:set,MOZILLA;flowbits:reset; sid:69; rev:2;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"Detect Mozilla Firefox browser "; flags:+PA,12; pcre:"/(GET|POST|HEAD)/m"; content:"HTTP/1."; content:"Accept"; content:"Host"; nocase; content:"User-Agent:";nocase;content:"Mozilla/5"; content:"Firefox/"; flowbits:isset,ACK; flowbits:set,Moz;flowbits:reset; sid:70; rev:2;)

##

#drop tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"drop if not Browser IE6 or Firefox winxpi or Firefox "; flags:+PA,12;flowbits:isnotset,IE|MOZILLA|Moz; sid:72;rev:2;)

4.8.7 What2evade

Penulisan peraturan bagi mengesan What2evade melibatkan susunan aliran dari sesi 1 ke sesi 2 yang kemudian dihentikan oleh IPS . Dalam hubungan ini, selepas 3 *way handshake* berlaku, penulisan peraturan bagi proses deteksi oleh IPS melibatkan susunan sesi 1 serta diikuti oleh sesi ke 2 dan menggugurkan sebarang sesi selepas itu seperti yang dizahirkan melalui Rajah di bawah. Peraturan ini juga boleh digunapakai untuk sebarang pencerobohan yang menggunakan *multiple session per stream*.

Copyright@FTSM

#3 handshake flow

alert tcp $EXTERNAL_NET any -> $HOME_NET [80,443] (msg:"alert tcp.syn Syn"; flags: +S,12; flowbits:set,tcp.syn1; flowbits:noalert;sid:55; rev:2;)

alert tcp $HOME_NET [80,443] -> $EXTERNAL_NET any (msg:"alert Syn-Ack from server"; flags: +SA,12; flowbits:isset,tcp.syn1; flowbits:set,syn-ack;flowbits:noalert; sid:56; rev:2;)

alert tcp $EXTERNAL_NET any -> $HOME_NET [80,443] (msg:"alert tcp Ack flags from client"; flags: !SRPUF,12; flowbits:isset,syn-ack;flowbits:set,ACK;flowbits:noalert;flowbits:reset; sid:57; rev:2;)

##

##detect flow from HTTP with GET/POST

alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"HTTP client flow 1 "; flags:+PA,12; pcre:"/(GET|POST|HEAD)/m"; content:"HTTP/1."; content:"Accept"; content:"Host"; nocase; content:"User-Agent:";nocase; flowbits:isset,ACK; flowbits:set,flow1; sid:988; rev:2;)

alert tcp $HOME_NET 80 -> $EXTERNAL_NET any (msg:"response flow 1"; content:"HTTP/1"; content:"200 OK" ; flowbits:isset,flow1;flowbits:set,flow2;flowbits:reset;sid:81;rev:2;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"HTTP client flow 2 "; flags:+PA,12; pcre:"/(GET|POST|HEAD)/m"; content:"HTTP/1."; content:"Accept"; content:"Host"; nocase; content:"User-Agent:";nocase; flowbits:isset,flow2;flowbits:set,flow3; sid:977; rev:2;)

drop tcp $HOME_NET 80 -> $EXTERNAL_NET any (msg:"drop response flow 2"; content:"HTTP/1"; content:"200 OK" ; flowbits:isset,flow3;flowbits:reset;sid:89;rev:2;)

##

5. KESIMPULAN

5.1 Latar Belakang

Kajian ini telah meliputi teknik penyusupan data melalui fungsi pintasan (*bypass*), terowongan (*tunneling*) , cangkerang songsang (*reverse shell*) serta cangkerang ikatan (*bind shell*) melalui protokol HTTP menggunakan *aplikasi (tools)* seperti Fireaway, Badcookies, Cookiesmaster, DET, HTTyHole, Data Exfiltration_HTTP, Firedrill dan What2evade menggunakan senario *post exploitation.* Melalui kajian ini juga, kesemua *aplikasi (tools)* yang digunakan berjaya melepasi tahap keselamatan asas sistem organisasi.

Asas dalam kajian ini adalah mengkaji karektor muat beban *(payload)* yang terlibat bagi memudahkan pengenalpastian sekaligus memudahkan IT personel untuk merangka *rules*

Copyright@FTSM

bagi mengekang kemasukan yang sama berlaku di peringkat IPS. Dalam melaksanakan kajian ini, dikesan tiga (3) perkara yang perlu diberi penekanan iaitu :

i. Penekanan (*weightage*) perlu difokuskan kepada pemulihan pasca penyusupan. Kebanyakan pendekatan menumpukan kepada pengesanan, pencegahan dan mitigasi. Walau bagaimanapun, tidak ada penyelesaian yang holistik dikesan bagi mendapatkan keselamatan memandangkan persekitaran korporat yang semakin kompleks. Pemulihan itu wajar menjadi tumpuan utama strategi, alat dan teknik bagi menangani ancaman penyusupan keluar data.

ii. Pendekatan semasa yang menjadi amalan termasuk sistem komersil lebih mengutamakan kepada dasar spesifikasi serta pelaksanaan terhadap langkah-langkah pencegahan seperti menggugurkan semua saluran sulit seperti ssh ekoran ianya tidak boleh dikaji oleh IDS. Namun demikian, langkah-langkah yang diambil mungkin memberikan solusi tempoh pendek namun ianya tidak dapat digarap secara efektif di dalam persekitaran amalan kerja bagi memastikan ia kekal relevan.

iii. Fokus perlu ditukarkan daripada ―Perlindungan Maklumat‖ kepada ―Pengesanan dan Pencegahan Penyusupan Keluar Data – memandangkan kompleksiti organisasi dan senario hypermobiliti terkini. Pendirian ini dilihat lebih holistik dan mampu menangani ancaman serta mengurus isu berkaitan tahap kritikal data.

Pada masa yang sama, memandangkan kajian ini hanya menggunakan tujuh (7) instrumen penyusupan keluar data dan menumpukan kepada protokol HTTP sahaja, dilihat masih ada ruang untuk kajian di masa hadapan untuk menggunakan instrument lain di pasaran dan juga protokol yang berbeza untuk mengkaji dan menganalisa fitur paket.

5.2 Rumusan

Pengesanan awal adalah kritikal dalam mengekang penggodam dari melakukan penyusupan keluar data. Di sini letaknya kepentingan bagi organisasi untuk membangunkan risikan terhadap ancaman (*threat intelligence*) dalam mengekang serta mengesan sebarang aktiviti berkaitan APT. Pemantauan berterusan bersama modal insan yang mantap dalam mengenalpasti anomali di dalam paket adalah kunci dalam pengurusan keselamatan data. Satu lagi aspek pencegahan penyusupan adalah dalam penentuan dan penguatkuasaan dasar keselamatan berkaitan dengan pemberian dan pengekalan akses terhadap data sensitif.

Copyright@FTSM

RUJUKAN

Abd Rahman, A. R. 2006. Democracy and the public sphere: consequences of ICT policy in Malaysia / Abd Rasid Abd Rahman.

Antwerp, R. C. . Van. 2011. Exfiltration Techniques : An Examination and Emulation.

Berk, V., Giani, A. & Cybenko, G. 2005. Detection of Covert Channel Encoding in Network Packet Delays.

Born, K. 2010. *PSUDP: A passive approach to network-wide covert communication. Black Hat USA,*.

Bossler, A. M. & Burrus, G. W. 2011. The General Theory of Crime and Computer Hacking : low Self Control Hackers? *Corporate Hacking and Technology-Driven Crime,* hlm.39–67. New York: Information Science Reference.

Brenner, S. W. 2009. *Cyberthreats: The Emerging Fault Lines of the Nation State*. doi:10.1093/acprof:oso/9780195385014.001.0001

Bruce Schneier. 2010. Schneier on Security. *Forbes*,.

Choe Sang-Hun. 2013. Cyberattack Hits South Korean Banking Networks - The New York Times. *New York Times*,. http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html?_r=0 [14 August 2016].

Choi, M., Robles, R. J., Hong, C. & Kim, T. 2008. Wireless Network Security : Vulnerabilities , Threats and Countermeasures. *International Journal of Multimedia and Ubiquitous Engineering*, *3*(3), 77–86.

CISCO. 2015. Network as a Security Sensor Threat Defense with Full NetFlow 1–19.

Cody, B. 2015. Data Exfiltration Demystified — Actors , Tools , and Techniques. *FOCUS 15th Security Conference*,. Las Vegas.

Dahlgren, P. 2005. The Internet, Public Spheres, and Political Communication: Dispersion and Deliberation. *Political Communication*, *22*(2), 147–162. doi:10.1080/10584600590933160

Dambala Inc. 2013. *Stopping an Infection from Becoming a Breach*.

Dan Munro. 2015. Data Breaches In Healthcare Totaled Over 112 Million Records In 2015. *Forbes*,. http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#27bfa89b7fd5 [13 September 2016].

Dave Lee. 2012. Flame: Massive cyber-attack discovered, researchers say - BBC News. *BBC News*,. http://www.bbc.com/news/technology-18238326 [18 May 2017].

Denning, D. E. 2011. Cyber Conflict as an Emergent Social Phenomenon. *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, hlm.170–186. New York: Information Science Reference. doi:10.4018/978-1-61692-805-6.ch009

Dlamini, M. T., Eloff, J. H. P. & Eloff, M. M. 2009. Information security: The moving target. *Computers & Security*, *28*(3–4), 189–198. doi:10.1016/j.cose.2008.11.007

Dutt, V., Ahn, Y.-S. & Gonzalez, C. 2013. Cyber situation awareness: modeling detection of cyber attacks with instance-based learning theory. *Human factors*, *55*(3), 605–18. doi:10.1177/0018720812464045

E-Isac. 2016. Analysis of the Cyber Attack on the Ukrainian Power Grid 29.

Ekonomi, P. 2014. Prestasi Ekonomi dan Prospek 1–62.

Fallis, A. . 2013. Data Exfiltration: How Do Threat Actors Steal Your Data? *Data Exfiltration*, *53*(9), 1689–1699. doi:10.1017/CBO9781107415324.004

Fawcett, T. W. 2010. *Exfild : a Tool for the Detection of Data Exfiltration Using Entropy and Encryption Characteristics of Network Traffic*. University of Delaware.

FireEye Industry Inc. 2016. Cyber Attacks on the Ukrainian Grid: What You Should Know.

Fraga, D., Banković, Z. & Moya, J. M. 2012. A taxonomy of trust and reputation system attacks. *Proc. of the 11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012 - 11th IEEE Int. Conference on Ubiquitous Computing and Communications, IUCC-2012*, 41–50. doi:10.1109/TrustCom.2012.58

Geers, K., Kindlund, D., Moran, N. & Rachwald, R. 2015. FireEye World War C : Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks (April).

Giani, A., Berk, V. H. & Cybenko, G. V. 2006. Data exfiltration and covert channels. *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense V*, 620103-620103–11. doi:10.1117/12.670123

Goode, A. 2010. Managing mobile security: How are we doing? *Network Security*, *2010*(2), 12–15. doi:10.1016/S1353-4858(10)70025-8

Guri, M., Solewicz, Y., Daidakulov, A., Elovici, Y. & Security, C. 2016. DiskFiltration: Data

Copyright@FTSM

Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise.

Hermans, J. 2013. The five most common cyber security mistakes : Management ' s perspective on cyber security.

Holt, T. J. 2007. Subcultural Evolution?: Examining The Influence of On and Offline Experiences On Deviant Subcultures. *Deviant Behavior*, *28*(2), 171–198. doi:10.1080/01639620601131065

Holt, T. J. 2012. Examining willingness to attack critical infrastructure online and offline. *Crime and delinquency*, *58*(5), 798–822. doi:http://dx.doi.org/10.1177/0011128712452963

Holt, T. J. 2013. *Crime On-Line : Correlates , Causes and Context*. Durham: Carolina Academia Press.

Holt, T. J. & Schell, B. H. 2011. Corporate Hacking and Technology-Driven Crime : Social Dynamics and Implications. *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*,. New York: Information Science Reference. doi:10.4018/978-1-61692-805-6

Information Is Beautiful.Net. 2017. World's Biggest Data Breaches & Hacks — Information is Beautiful. http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ [12 April 2017].

InfoSec Institute. 2015. Duqu 2.0: The Most Sophisticated Malware Ever Seen. *InfoSec Institute*,. http://resources.infosecinstitute.com/duqu-2-0-the-most-sophisticated-malware-ever-seen/#gref [18 May 2017].

Kilger, M. 2011. Social Dynamics and the Future of Technology-Driven Crime. *Corporate Hacking and Technology-Driven Crime*, hlm.205–227. doi:10.4018/978-1-61692-805-6.ch011

Koeppen, E. 2014. How they're getting the data out of your network.

Kotulic, A. & Clark, J. 2004. Why there aren't more information security research studies. *Information & Management*,.

Laventhal, R. 2016. Massive Cyber Attack at Banner Health Affects 3.7M Individuals | Healthcare Informatics Magazine | Health IT | Information Technology. http://www.healthcare-informatics.com/news-item/cybersecurity/breaking-massive-cyber-attack-banner-health-affects-37m-individuals

Lough, D. L. 2001. A Taxonomy of Computer Attacks with Applications to Wireless Networks (April), 1–373.

Mancuso, V. F., Strang, A. J., Funke, G. J. & Finomore, V. S. 2014. Human Factors of Cyber Attacks: A Framework for Human-Centered Research. *Proceedings of the Human Factors and Ergonomics Society 58th Annual Meeting*, (2012), 437–441. doi:10.1177/1541931214581091

Marjie T. Britz. 2010. Terrorism and technology: Operationalizing cyberterrorism and identifying concepts.

Miranda, M. 2011. Detecting Data Exfiltration Exfiltrations are Happening.

Neal Harris. 2013. Black Hat 2013 - SSL, Gone in 30 Seconds - A BREACH beyond CRIME - YouTube.

Obszyński, A. 2015. Infoblox DNS Threat Insight & DNS Firewall Time to control DNS – for You , for Your subscribers and Your users !

Payer, M. 2014. HexPADS : a platform to detect ― stealth ‖ attacks.

Potter, B. 2011. Coming to grips with security. *IT Professional*, *13*(3), 14–16. doi:10.1109/MITP.2011.39

Rashid, A., Ramdhany, R., Edwards, M., Kibirige, S. M., Babar, A., Hutchison, D. & Chitchyan, R. 2013. Detecting and Preventing Data Exfiltration. *Security Lancester*,.

Reuters. 2016. Bangladesh Bank - Fortune. http://fortune.com/tag/bangladesh-bank/

Copyright@FTSM

Ruhiu, N. D. 2013. Data Exfiltration In Organizations (December).

Seals, T. 2017. Insider Threats Responsible for 43% of Data Breaches - Infosecurity Magazine. *Info Security Europe edition*,. https://www.infosecurity-magazine.com/news/insider-threats-reponsible-for-43/ [26 April 2017].

Unit Perancang Ekonomi. 2016. Laporan Tahunan Program Transformasi Negara 2015. *Edisi Pertama, Percetakan Pertama 2016*, (2180–294), 290. doi:10.1017/CBO9781107415324.004

V Jyothsna, V V Rama Prasad & Munivara K Prasad. 2013. A Review of Anomaly Based Intrusion Detection System. *International Journal of Computer Applications*, *68*(24), 7–11. doi:10.5120/11725-7304

Verizon. 2016. 2016 Data Breach Investigations Report. *Verizon Business Journal*, (1), 1–65. doi:10.1017/CBO9781107415324.004

Villeneuve, N. & Bennett, J. 2012. *Detecting APT Activity with Network Traffic Analysis*. *Trend Micro*,.

Wahab, A. 2016. Securing Critical Systems for Protection of National Digital Assets (April).

Wendzel, S. 2014. The Future of Data Exfiltration and malicious communication. https://www.youtube.com/watch?v=KE8oWpU6l9o [10 April 2017].

Zetter, K. 2014. An Unprecedented Look at Stuxnet, the World's First Digital Weapon | WIRED. *Wired*,. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ [18 May 2017].

Copyright@FTSM