PENGESANAN PERISIAN HASAD: PENGGUNA AKHIR MENERUSI MESIN MAYA, KOTAK PASIR DALAM TALIAN DAN FUZZY HASHING

SOO WENG JYH

UNIVERSITI KEBANGSAAN MALAYSIA

PENGESANAN PERISIAN HASAD: PENGGUNA AKHIR MENERUSI MESIN MAYA, KOTAK PASIR DALAM TALIAN DAN FUZZY HASHING

SOO WENG JYH

PROJEK YANG DIKEMUKAKAN UNTUK MEMENUHI SEBAHAGIAN
DARIPADA SYARAT MEMPEROLEHI IJAZAH
SARJANA KESELAMATAN SIBER

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2023

PENGAKUAN

Saya akui karya ini adalah hasil kerja saya sendiri kecuali nukilan dan ringkasan yang tiap-tiap satunya telah saya jelaskan sumbernya.

22 Ogos 2023

SOO WENG JYH
P117259

PENGHARGAAN

Dengan penuh penghargaan, saya ingin merakamkan setinggi-tinggi terima kasih kepada Prof. Madya Dr. Khairul Akram bin Zainol Ariffin sebagai penyelia saya. Beliau telah memberikan tunjuk ajar, bimbingan, dan komen yang penuh pemikiran dan kritikan membina, yang sangat membantu membentuk dan menjadikan karya ini lebih teliti dan mendalam. Bimbingan, sokongan, kesabaran, dorongan, dan maklum balas yang tidak ternilai daripada beliau sepanjang proses penyelidikan dan penulisan tesis ini telah menjadi faktor penting dalam membantu saya mengembangkan ide dan menghasilkan karya yang saya banggakan.

Saya juga ingin mengucapkan penghargaan kepada Dr. Wandeep Kaur A/P Ratan Singh sebagai Penyelaras Program (Sarjana mengikut Modul) serta semua pensyarah dan kakitangan Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia, yang telah memberikan banyak bantuan kepada saya dalam setiap modul, baik secara langsung mahupun tidak langsung, dalam menyiapkan kajian ini dalam jangka masa yang ditetapkan untuk menyempurnakan pengajian sarjana saya.

Akhirnya, terima kasih yang tak terhingga saya ucapkan kepada isteri saya Kam Fong Yee, anak saya Soo Ming Hui, ahli keluarga sekalian, dan rakan-rakan seperjuangan (Zhang LuLu, Teo Wei Chen, Foo Jia Yung dan lain-lain) atas galakan yang mereka berikan dalam menyelesaikan kajian ini. Sumbangan dan jasa yang diberikan oleh mereka akan sentiasa dikenang dan terukir dalam hati saya. Saya berharap kajian ini dapat memberikan sumbangan yang berharga dalam bidang yang dikaji dan menjadi rujukan bagi para pengkaji di masa depan.

ABSTRAK

Perisian hasad merupakan ancaman dalam landskap digital masa kini yang menembusi ke pelbagai saluran komunikasi dan menyebabkan kerosakan. Antara yang paling rentan adalah pengguna akhir, yang seringkali menjadi mangsa perisian hasad tanpa disedari seperti klik tanpa sengaja pada pautan berbahaya atau membuka fail tercemar. Akibatnya, perkakasan mereka menjadi terjejas dengan ancaman siber. Walau bagaimanapun, kemunculan kotak pasir perisian hasad telah membolehkan pengguna akhir menguji fail yang mencurigakan sebelum berlakunya jangkitan. Namun begitu, kotak pasir perisian hasad ini selalunya memerlukan tahap pengetahuan teknikal yang tinggi untuk melakukan konfigurasi yang tepat kerana melibatkan prosedur penyediaan yang kompleks. Oleh itu, kajian ini bertujuan mengatasi cabaran ini dengan meneroka penggunaan mesin maya (Flare VM) bersama dengan kotak pasir dalam talian (VirusTotal) yang tersedia secara percuma untuk menyiasat fail yang mencurigakan. Projek ini mendapati faktor yang berkaitan dengan manusia adalah titik lemah dalam keselamatan siber. Dengan eksperimen menggunakan mesin maya dan kotak pasir dalam talian, pengguna akhir dapat melakukan analisis statik dan dinamik untuk mengesan fail yang tidak diketahui, akhirnya menyumbang kepada peningkatan keseluruhan pengesanan perisian hasad. Banyak kotak pasir perisian hasad dalam talian sekarang menggabungkan fuzzy hashing (SSDEEP), membolehkan pengguna akhir mengenal pasti pelbagai variasi perisian hasad dengan lebih efektif. Kajian ini memperkasa pengguna akhir terutamanya pengguna akhir yang bekerja di Perusahaan Kecil dan Sederhana (PKS), memperkemas proses menguji fail yang mencurigakan dan mengukuhkan pertahanan terhadap landskap perisian hasad yang sentiasa berkembang. Oleh itu, projek ini dapat menyumbang dalam MyDigital (Rangka Tindakan Ekonomi Digital Malaysia) Teras 6 bagi menggalak PKS dalam membina persekitaran digital yang dipercayai, selamat dan beretika.

MALWARE DETECTION: END USER LEVERANGING VIRTUAL MACHINE, ONLINE SANDBOX AND FUZZY HASHING

ABSTRACT

Malware remains a significant threat in today's digital landscape, infiltrating various communication channels and causing significant damage. Among the most vulnerable targets are end-users, who often fall victim to malware without even realizing it—perhaps by accidentally clicking on malicious links or opening contaminated files. As a result, their hardware becomes susceptible to cyber threats. However, the emergence of sandboxed malware analysis has allowed end-users to test suspicious files before infections occur. Nevertheless, configuring sandbox environments often requires a high level of technical expertise due to their complex setup procedures. This study aims to address this challenge by exploring the use of virtual machines like Flare VM in conjunction with online sandboxes like VirusTotal, both freely available, to investigate suspicious files. The project finds that human factors are weak points in cybersecurity, as evidenced by a review of the existing literature. Through experiments using virtual machines and online sandboxes, end-users can conduct static and dynamic analyses to detect unknown malware effectively, ultimately contributing to overall malware detection improvement. Many online sandbox environments now incorporate fuzzy hashing (SSDEEP), enabling end-users to identify various malware variations more efficiently. The value of this research lies in empowering end-users, particularly those in Small and Medium-sized Enterprises (SMEs), by strengthening the process of testing suspicious files and fortifying defenses against the ever-evolving malware landscape. Consequently, this project aligns with MyDigital (Malaysia Digital Economy Blueprint) Core Thrust 6, which encourages SMEs to build trusted, secure, and ethical digital environments.

KANDUNGAN

Halaman

SENARAI JADUAL

SENARAI ILUSTRASI

SENARAI SINGKATAN

APWG	Anti-Phishing Working Group
CSM	CyberSecurity Malaysia
CPU	Central Processing Unit
FTSM	Fakulti Teknologi dan Sains Maklumat
KDNK	Keluaran Dalam Negara Kasar
MCSS	Malaysia Cyber Security Strategy
MKN	Majlis Keselamatan Negara
MyCERT	Malaysia Computer Emergency Response Team
NACSA	National Cyber Security Agency
NIST	National Institute of Standards and Technology
OS	Operating System
OVF	Open Virtualization Format
PDRM	Polis Diraja Malaysia
PKS	Perusahaan Kecil dan Sederhana
PUA	Potentially Unwanted Application
RAM	Random Access Memory
SKMM	Suruhanjaya Komunikasi dan Multimedia Malaysia
SME	Small and Medium-sized Enterprise
UKM	Universiti Kebangsaan Malaysia
VHD	Virtual Hard Disk
VM	Virtual Machine

BAB I

PENDAHULUAN

1.1 PENGENALAN

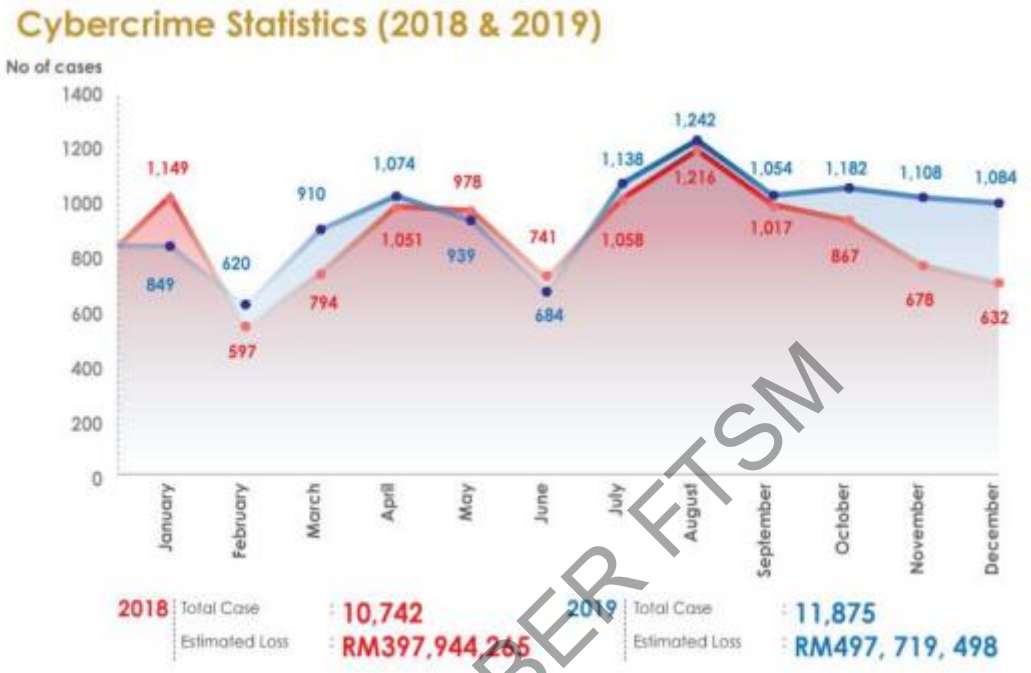
Perisian hasad (malware) semakin berkembang secara sofistikated, menjadikan pengguna akhir mudah terperangkap dalam perangkap kejuruteraan sosial. Oleh itu, adalah penting bagi pengguna akhir untuk memanfaatkan mesin maya (virtual machine), kotak pasir perisian hasad dalam talian (online malware sandbox), dan fuzzy hashing untuk mengkaji fail-fail yang tidak diketahui. Pengguna akhir dapat menggunakan kotak pasir perisian hasad dalam talian yang tersedia secara awam sebagai gantian kepada pengaturan manual yang rumit. Dengan ini, pengguna akhir dapat membantu sebagai pembela pertama dan menyumbang kepada komuniti dalam memerangi perisian hasad ini.

1.2 LATAR BELAKANG KAJIAN

Pada masa sekarang, ancaman daripada perisian berbahaya semakin rumit dan sukar dikesan oleh perisian keselamatan sedia ada. Penjenayah siber semakin menggunakan kaedah kejuruteraan sosial yang canggih untuk memanipulasi pengguna agar mengklik pautan yang berbahaya atau memuat turun fail yang mengandungi perisian hasad. Pengguna sering kali terperangkap tanpa sedar yang membawa kepada implikasi keselamatan dan privasi yang serius.

Dalam laporan Strategi Keselamatan Siber Malaysia 2020-2024 (NACSA, 2020), Unit Jenayah Digital Microsoft Asia menganggarkan bahawa setiap minit, 720 orang di seluruh dunia menjadi mangsa penjenayah siber, berjumlah lebih daripada 1 juta mangsa setiap hari. Pada tahun 2018, Polis Diraja Malaysia menangani 10,742 kes jenayah siber dengan kerugian melebihi RM400 juta, manakala dijangkakan terdapat

11,875 kes dengan kerugian hampir RM500 juta pada tahun 2019. Rajah 1.1 menunjukan statistik jenayah siber bagi tahun 2018 & 2019

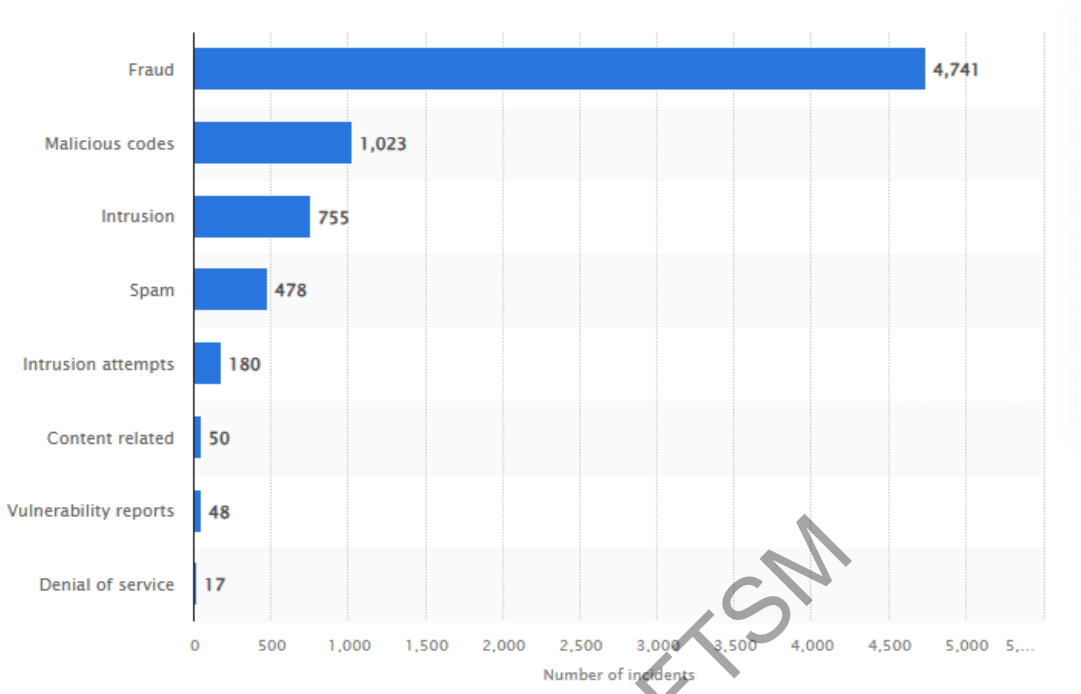


Rajah 1.1 Statistik Jenayah Siber (2018 & 2019)

Sumber: (Majlis Keselamatan Negara(MKN), n.d.)

Selain itu, laporan Strategi Keselamatan Siber Malaysia 2020-2024 menganggarkan bahawa Malaysia berisiko kehilangan sehingga RM51 bilion dalam output ekonomi disebabkan oleh insiden keselamatan siber, atau lebih daripada 4% daripada KDNK (Keluaran Dalam Negara Kasar) negara secara keseluruhan. (“Majlis Keselamatan Negara(MKN),” n.d.)

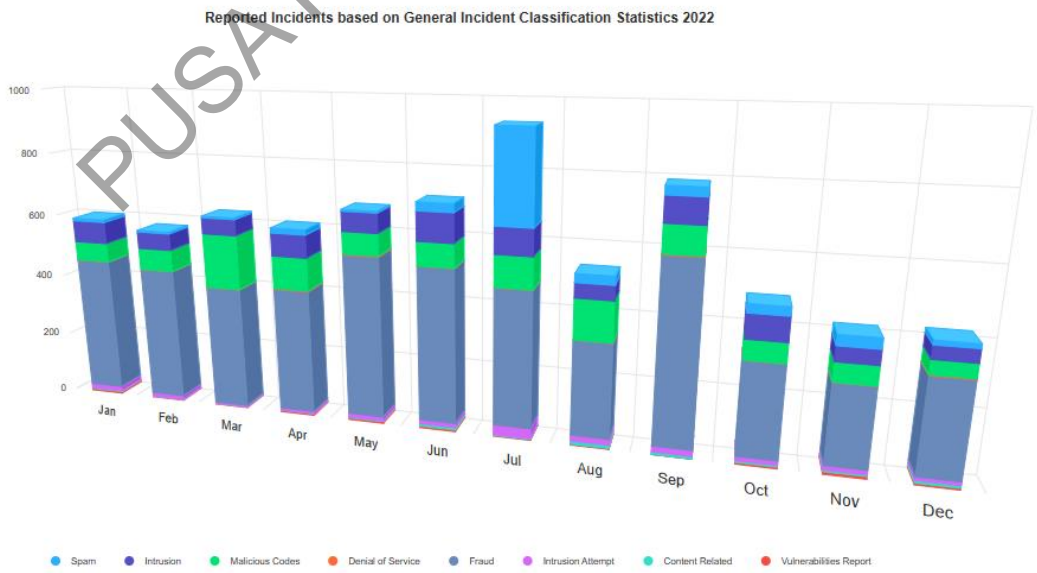
Jabatan Penyelidikan Statista (2023) menerbitkan bahawa penipuan dalam talian merupakan insiden ancaman siber paling banyak dilaporkan dengan lebih daripada empat ribu laporan, diikuti oleh kod jahat pada tahun 2022 (Rajah 1.2).



Rajah 1.2 Malaysia: Insiden Jenayah Siber 2022

Sumber: (Malaysia: Cyber Crime Incidents 2018, n.d.)

MyCERT (2023) menyediakan statistik terperinci mengenai insiden yang dilaporkan berdasarkan pengelasan insiden secara umum untuk tahun 2022. (Rajah 1.3)



bersambung…

…sambungan

#	JAN	FEB	MAC	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Spam	8	5	6	15	7	27	286	27	27	27	31	12	478
Intrusion	68	54	50	74	59	89	82	45	76	73	44	41	755
Malicious Codes	62	68	174	103	70	75	98	124	86	61	60	42	1,023
Denial of Service	0	2	1	1	4	2	0	1	3	2	0	1	17
Fraud	431	423	388	396	509	486	429	294	566	285	244	290	4,741
Intrusion Attempt	15	12	4	6	15	14	32	21	20	15	13	13	180
Content Related	2	0	0	2	2	7	1	10	7	5	6	8	50
Vulnerabilities Report	6	3	3	4	5	5	3	2	0	5	8	4	48
	592	567	626	601	671	705	931	524	785	473	406	411	7,292

Rajah 1.3 MyCERT : Statistik Kejadian - Kejadian Dilaporkan Berdasarkan Statistik Klasifikasi Insiden Am 2022

Sumber: (MyCERT : Incident Statistics - Reported Incidents Based on General Incident Classification Statistics 2022, n.d.)

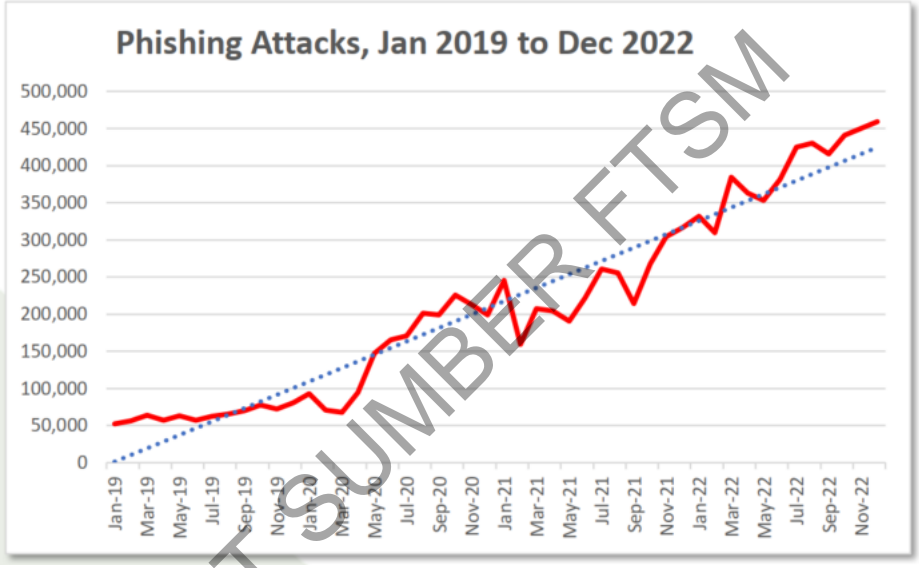
Apabila pengguna akhir menghadapi fail yang tidak diketahui, terdapat beberapa tindakan yang boleh mereka ambil. Pertama, mereka boleh menjalankan fail tersebut dalam persekitaran mesin maya atau kotak pasir perisian hasad untuk analisis statik dan dinamik. Analisis statik melibatkan pemeriksaan fail untuk mengenal pasti tanda-tanda jangkitan, seperti kod berbahaya atau perilaku mencurigakan. Analisis dinamik pula melibatkan menjalankan fail dalam persekitaran terkawal untuk mengesan aktiviti berbahaya semasa pelaksanaannya.

Selepas itu, mereka boleh menggunakan perkhidmatan kotak pasir perisian hasad dalam talian yang disediakan oleh pelbagai pihak untuk menjalankan analisis lanjutan. Dalam kotak pasir perisian hasad, fail akan dijalankan dalam persekitaran yang berasingan dan disekat untuk mengesan tingkah laku jahat dan potensi ancaman.

Selain itu, pengguna akhir juga boleh merujuk kepada teknik fuzzy hashing untuk membandingkan fail yang tidak diketahui dengan ciri-ciri fail perisian hasad yang telah diketahui. Ini boleh membantu mengenal pasti jika fail tersebut merupakan varian baru daripada keluarga perisian hasad yang sedia ada.

Selain tindakan teknikal, pengguna akhir juga dapat membantu melawan perisian hasad dengan berkongsi maklumat dan laporan mengenai fail yang tidak diketahui dengan komuniti keselamatan siber, seperti MyCERT atau pihak berkuasa yang berkaitan. Dengan berbuat demikian, mereka turut menyumbang kepada upaya pengesan perisian hasad secara keseluruhan dan melindungi pengguna lain dari ancaman yang serupa.

1.3 PENYATAAN MASALAH



Rajah 1.4 Ancaman Phishing, Jan 2019 to Dec 2022

Sumber: APWG | Phishing Activity Trends Reports, 2019

Melihat sepanjang empat tahun seperti di Rajah 1.4, Anti-Phishing Working Group (APWG) telah menyaksikan peningkatan yang ketara dalam ancaman phishing, mempercepatkan kepada lebih daripada 150% setahun (APWG | Phishing Activity Trends Reports, 2019). Berdasarkan statistik yang diberikan, ini menunjukkan bahawa manusia kekal sebagai sasaran utama kerana phishing merupakan suatu jenayah siber yang melibatkan kejuruteraan sosial untuk mencuri data identiti peribadi pengguna dan akaun kewangan. Skim kejuruteraan sosial memperdayakan pengguna akhir terperangkap ke laman sesawang palsu untuk mendedahkan data kewangan seperti nama pengguna dan kata laluan atau memasang perisian hasad ke dalam komputer pengguna akhir. Menurut kepada Desolda et al., 2021, phishing adalah sejenis serangan

siber yang sering berjaya kerana pengguna tidak menyedari kelemahan mereka atau tidak dapat memahami risiko.

Tinjauan 2019 oleh syarikat insurans Hiscox menunjukkan peningkatan serangan siber terhadap perniagaan di Britain, dengan 55% perniagaan dilaporkan menghadapi serangan pada tahun tersebut, berbanding dengan 40% pada tahun sebelumnya. Perniagaan Kecil dan Sederhana (PKS) juga tidak terkecuali daripada ancaman siber tersebut, dan saiz mereka yang lebih kecil membuat mereka lebih rentan sebagai sasaran yang menonjol. Menurut Cyber Security Breaches Survey 2019, meskipun 78% PKS menganggap keselamatan siber sebagai keutamaan tinggi; tetapi hanya 15% yang memiliki proses pengurusan insiden siber formal, menunjukkan jurang antara kesedaran dan tindakan yang diambil dalam menghadapi risiko siber (Lloyd, 2020).

Dalam kajian Zimmermann & Renaud (2019), penyelidikan mereka mendapati bahawa pengesanan dan pengenalpastian insiden bergantung kepada pelaporan manusia atau pelaporan yang dibantu oleh manusia. Ini menunjukkan bahawa manusia memainkan peranan penting dalam kejayaan keselamatan siber. Selain itu, membatasi atau mengecualikan peranan manusia dari sistem bermakna kita membatasi kesilapan, tetapi juga menghadkan kemampuan semua individu manusia untuk menyumbang secara aktif dalam menjaga dan meningkatkan keselamatan. Pelaku manusia perlu diberi ruang untuk penyertaan dalam usaha keamanan (Zimmermann & Renaud, 2019).

Kajian oleh Kamal et al., 2021 menunjukkan bahawa kotak pasir Cuckoo berdasarkan sistem operasi Linux, sukar memasang dan mengkonfigurasi awal tanpa ilmu komputer. Contohnya, kerumitan yang terlibat dalam menubuhkan kotak pasir perisian hasad memberikan halangan penting bagi pengguna akhir yang berusaha membina persekitaran kotak pasir mereka sendiri. Kerumitan ini menghalang keupayaan mereka untuk mencipta dan menggunakan sistem kotak pasir dengan berkesan, mengehadkan keupayaan mereka untuk menganalisis dan mengurangkan potensi ancaman.

Dalam arena keselamatan siber, laporan Microsoft mengakui bahawa manusia sering dianggap sebagai titik lemah dalam keselamatan, tetapi juga bahawa dengan latihan dan pendidikan, mereka juga boleh menjadi barisan pertahanan pertama. Sebagai contoh, mereka menjelaskan bagaimana pekerja yang mengesan dan melaporkan e-mel yang mencurigakan dapat menghentikan serangan penipuan phishing. (Zimmermann & Renaud, 2019)

Pawlicka et al., 2022 telah dikaji bahawa dalam usaha mempertingkatkan keselamatan siber, organisasi dan pakar perlu sedar bahawa fokus tidak boleh hanya tertumpu kepada penyelesaian teknikal semata-mata, dan melabur berjuta-juta dolar dalam melaksanakan teknologi tanpa menilai keupayaan pekerja; tanpa kerjasama, pemahaman, dan sokongan pekerja.

Faktor manusia menimbulkan cabaran besar dalam menangani perisian hasad, menjadikannya pautan lemah dalam rantaian keselamatan. Tingkah laku manusia, termasuk kurang kesedaran, kelemahan terhadap taktik kejuruteraan sosial, dan kesilapan dalam penghakiman, sangat menyumbang kepada kejayaan serangan perisian hasad.

1.4 PERSOALAN KAJIAN

Berdasarkan penyataan masalah yang telah dikenal pasti, persoalan kajian adalah seperti berikut:

1. Apakah faktor yang mempengaruhi pengguna akhir terhadap kesediaan keselamatan siber?

2. Bagaimanakah pengguna akhir boleh memanfaatkan mesin maya dan kotak pasir perisian hasad dalam talian untuk meningkatkan keberkesanan dan ketepatan pengesanan perisian hasad?

1.5 OBJEKTIF KAJIAN

Oleh itu, projek ini akan menumpukan kepada objektif seperti berikut:

1. Mengenal pasti faktor-faktor kesediaan keselamatan siber oleh pengguna akhir

2. Membangunkan langkah asas untuk pengguna akhir berdasarkan rangka kerja keselamatan siber NIST

1.6 SKOP KAJIAN

Skop penyelidikan ini memberi tumpuan kepada meneroka faktor-faktor yang menjadikan pengguna akhir sebagai titik lemah dalam keselamatan siber, dan cabaran dalam membina kotak pasir perisian hasad sendiri. Kajian ini akan mendorong pengguna akhir untuk memanfaatkan mesin maya yang lebih mudah dibina dan menggunakan kotak pasir perisian hasad dalam talian yang tersedia secara umum untuk menganalisis fail-fail yang tidak diketahui. Kajian ini akan membimbing pengguna akhir untuk mengikut Rangka kerja keselamatan siber NIST (National Institute of Standards and Technology) yang sedia ada bagi melaksanakan langkah-langkah secara praktikal.

Dalam projek ini, "Pengguna Akhir" ditakrifkan sebagai individu yang memiliki pengetahuan IT terhad dan pengalaman keselamatan siber yang terhad. Pengguna akhir ini boleh menjadi mana-mana pekerja yang bekerja di Perusahaan Kecil dan Sederhana (PKS). Pengguna akhir di sini tidak merujuk kepada pengamal atau pakar keselamatan siber.

1.7 KEPENTINGAN KAJIAN

Dalam projek ini, penyelidikan akan memberi tumpuan kepada pengguna akhir memanfaatkan mesin maya dan kotak pasir perisian hasad dalam talian untuk analisis perisian hasad dan peningkatan kesedaran keselamatan siber akan menjadi topik yang bernilai dan berguna kepada masyarakat.

Aplikasi praktikal: Penggunaan mesin maya dan kotak pasir perisian hasad dalam talian merupakan pendekatan yang berkesan untuk menganalisis fail-fail yang tidak diketahui dan mengesan potensi perisian hasad. Dengan menyelidik dan mempromosikan penggunaan alat-alat ini, kajian ini dapat memberikan panduan praktikal kepada pengguna akhir tentang bagaimana mereka dapat melindungi diri daripada ancaman perisian hasad.

Pemerkasaan Pengguna: Mendorong pengguna akhir untuk menggunakan mesin maya dan kotak pasir perisian hasad dalam talian memberi mereka keupayaan untuk mengambil peranan aktif dalam menganalisis fail yang mencurigakan dan mencegah serangan perisian hasad. Penyelidikan ini dapat membantu pengguna akhir mengembangkan kemahiran dan pengetahuan yang diperlukan untuk membuat keputusan yang berinformasi mengenai analisis fail dan amalan keselamatan siber.

Peningkatan Kesedaran: Dengan meningkatkan kesedaran tentang kepentingan keselamatan siber dan risiko yang berkaitan dengan fail-fail yang tidak diketahui, kajian ini menyumbang kepada persekitaran dalam talian yang lebih selamat. Penyelidikan ini dapat membantu mendidik pengguna akhir mengenai pelbagai teknik dan alat yang tersedia bagi mereka untuk pengesanan perisian hasad, dengan mempromosikan pendekatan proaktif terhadap keselamatan siber.

Peningkatan Pengesanan Perisian Hasad: Menganalisis keberkesanan mesin maya dan kotak pasir perisian hasad dalam talian dalam mengesan dan meredakan perisian hasad dapat memberikan pandangan yang berharga. Penyelidikan ini boleh melibatkan penilaian kejituan, kecekapan, dan batasan alat-alat ini, yang boleh menyumbang kepada pembangunan teknik pengesanan perisian hasad yang lebih baik.

1.8 ORGANISASI PENULISAN

Penulisan kajian ini terbahagi kepada lima bab seperti berikut:

Bab satu membincangkan dan menerangkan isu penggunaan siber yang melibatkan pengguna akhir. Bab ini juga menerangkan dengan lebih lanjut tentang latar

belakang kajian, penyataan masalah, persoalan kajian, objektif kajian, kepentingan kajian dan skop kajian.

Bab dua kajian ini adalah mengenai ulasan kepustakaan yang bertujuan untuk menjawab soalan-soalan penting yang berkaitan dengan kajian yang dijalankan. Bahagian pertama mengumpul cebisan kesusasteraan mengenai manusia adalah pautan lemah dalam keselamatan siber. Bahagian seterusnya membincangkan dan mengenal pasti alternatif seperti mesin maya dan kotak pasir perisian hasad dalam talian untuk membantu pengguna akhir dalam menyemak fail yang tidak diketahui. Bahagian terakhir adalah membangunkan rangka kerja konseptual seperti panduan praktikal untuk diikuti oleh pengguna akhir.

Bab tiga memperincikan mengenai metodologi atau kaedah bagaimana kajian ini dilaksanakan. Antara yang ditekankan dalam bab ini adalah tentang kaedah, prosedur dan teknik pengumpulan data yang diguna pakai dalam kajian. Selain itu, turut dibincangkan adalah populasi dan sampel kajian yang dipilih serta prosedur analisis data bagi kajian ini. Bab empat menerangkan mengenai kaedah analisis dan interpretasi data berdasarkan input dan maklumat yang diperolehi daripada ulasan kepustakaan. Hasil kajian ini menunjukkan bagaimana pengguna akhir disepadukan ke dalam Rangka Kerja Keselamatan Siber NIST, menekankan peranan mereka dan menonjolkan kesannya terhadap postur keselamatan siber PKS.

Bab lima menerangkan eksperimen terhadap perisian hasad menerusi mesin maya dan kotak pasir dalam talian. Keputusan eksperimen dan langkah-langkah dicadangkan kepada pengguna akhir akan dibincangkan. Bab enam menjelaskan tentang rumusan dapatan kajian, kekangan kajian, kesimpulan dan cadangan penambahbaikan untuk pelaksanaan kajian-kajian lain yang berkaitan di masa hadapan.

1.9 KESIMPULAN

Secara kesimpulannya, bab ini telah menggariskan pernyataan masalah yang dihadapi dalam kajian ini. Selain itu, dalam bab ini, soalan penyelidikan yang menjadi tumpuan kajian telah ditakrifkan dengan jelas. Soalan-soalan ini membantu memberi arah dan tujuan kajian untuk mencapai matlamat penyelidikan yang telah ditentukan.

BAB II

ULASAN KEPUSTAKAAN

2.1 PENGENALAN

Ulasan kepustakaan (Tesis & Ketiga, 2015) merupakan proses yang melibatkan penyelidikan semula ilmu pengetahuan dan kajian terdahulu, serta penilaian terhadap kemungkinan pelaksanaan kajian lanjutan. Kandungan teks dalam kajian ini telah mengikut templat dan panduan penulisan tesis Gaya UKM. (Templat Gaya UKM | Centre for Academic Management Cluster 2, 2016)

Di dalam ulasan kepustakaan ini, ia memberikan penilaian kritikal terhadap kesusasteraan sedia ada untuk mengenal pasti jurang, ketidakkonsistenan, dan bidang untuk penerokaan selanjutnya.

Proses penapisan kajian dan penulisan terdahulu dilakukan dengan teliti untuk memilih kajian yang relevan dengan persoalan kajian dan penyataan masalah. Ulasan kemudian melibatkan proses penyelidikan, pemahaman, dan penilaian terhadap hasil kajian dan penulisan terdahulu. Hasil penelitian dan penilaian kritis ini akan mengungkapkan bidang-bidang yang memerlukan peningkatan dan penyempurnaan. Selain itu, bab ini juga memberikan gambaran menyeluruh tentang persoalan kajian.

2.2 DEFINISI KONSEP UMUM

2.2.1 Pengguna Akhir

Dalam keselamatan siber, pengguna akhir merujuk kepada individu atau entiti yang menggunakan sistem komputer, rangkaian, aplikasi perisian, atau perkhidmatan digital. Mereka berperanan sebagai barisan pertahanan pertama terhadap ancaman dan kelemahan potensi. Pengguna akhir boleh termasuk pekerja, pengguna perkakasan

peribadi, pentadbir sistem, dan pengguna pihak ketiga. Kesedaran, pengetahuan, dan amalan keselamatan siber mereka adalah kritikal dalam memastikan persekitaran teknologi yang selamat dan berdaya tahan.

2.2.2 Perisian Hasad

Perisian Hasad, juga dikenali sebagai “Malware” dalam bahasa Inggeris, merujuk kepada perisian yang direka untuk merakam aktiviti pengguna tanpa kebenaran atau pengetahuan mereka. Ia berfungsi dengan mengumpul maklumat peribadi, aktiviti pelayar laman sesawang, kunci papan kekunci, atau melacak perilaku pengguna lain secara rahsia. Biasanya, perisian hasad digunakan dengan niat yang tidak bermoral atau jahat, seperti untuk mengintip privasi seseorang, mencuri maklumat sensitif, atau memantau kegiatan dalam talian.

Perisian hasad boleh disebarkan melalui pelbagai cara, termasuk melalui fail yang dimuat turun dari laman sesawang yang tidak dipercayai, melalui e-mel dengan lampiran berbahaya, atau melalui penyebaran tidak sah yang disertakan dalam aplikasi atau perisian lain. Ia sering kali berjalan secara tersembunyi di latar belakang sistem komputer atau peranti mudah alih tanpa pengetahuan pengguna.

Kesan perisian hasad boleh meliputi pencurian identiti, kehilangan maklumat peribadi, penyalahgunaan maklumat sensitif, atau merosakkan privasi dan keselamatan seseorang secara keseluruhan. Oleh itu, penting untuk melindungi diri daripada perisian hasad dengan menggunakan perisian keselamatan yang dikemas kini, mengelakkan memuat turun fail dari sumber yang tidak dipercayai, dan memastikan kehadiran alat keselamatan yang sesuai pada sistem komputer dan peranti mudah alih.

2.2.3 Perisian Virtualisasi

Perisian virtualisasi merujuk kepada perisian yang membolehkan pengguna mencipta dan menjalankan persekitaran maya atau mesin maya dalam komputer utama. Persekitaran maya ini berfungsi terasing dari sistem operasi utama komputer dan dapat meniru serta menjalankan sistem operasi dan aplikasi tambahan.

Dalam perisian virtualisasi, terdapat dua entiti utama yang terlibat: hipervisor dan mesin maya. Hipervisor bertanggungjawab mengurus dan mengawal akses kepada sumber daya peranti keras komputer serta menyediakan persekitaran yang terasing untuk mesin maya. Hipervisor boleh berupa perisian yang dijalankan di atas sistem operasi utama (hipervisor tumpukan) atau sebagai perisian asas yang beroperasi secara langsung pada peranti keras (hipervisor jenis 1).

Mesin maya pula adalah persekitaran maya yang dijalankan di atas hipervisor. Ia merangkumi sistem operasi maya dan perisian lain yang berjalan dalam persekitaran tersebut. Mesin maya menggunakan sumber daya komputer yang diberikan oleh hipervisor seperti CPU, memori, storan, dan peranti input-output.

Kelebihan utama perisian virtualisasi termasuk kemampuan menjalankan beberapa sistem operasi atau mesin maya secara selari di dalam satu komputer fizikal, memungkinkan aplikasi dan perisian yang tidak serasi dengan sistem operasi utama, serta menyediakan keadaan terkawal untuk pengujian dan pembangunan aplikasi dan sistem operasi.

Contoh perisian virtualisasi popular termasuk VirtualBox, VMware, dan Hyper-V, yang memungkinkan pengguna memanfaatkan kelebihan persekitaran maya untuk pengujian, pengembangan, konsolidasi, serta pengurusan dan pemberian perkhidmatan.

2.2.4 Mesin Maya

Mesin Maya, juga dikenali sebagai “Virtual Machine” dalam bahasa Inggeris, merujuk kepada persekitaran yang dikawal dan terasing yang digunakan untuk menjalankan perisian atau fail yang mencurigakan tanpa membahayakan sistem utama. Ia berfungsi sebagai persekitaran simulasi yang membolehkan penyelidik atau pengguna untuk menganalisis tingkah laku dan kesan perisian atau fail tersebut tanpa risiko kesan negatif ke atas sistem sebenar.

Dalam konteks keselamatan siber, mesin maya digunakan untuk mengkaji dan mengesan perisian berbahaya, termasuk perisian hasad. Dengan menjalankan perisian dalam persekitaran terkawal seperti mesin maya, pengguna dapat mengesan aktiviti

yang mencurigakan, mengkaji keupayaan perisian untuk menyebabkan kerosakan atau ancaman, dan mengumpul maklumat tentang taktik dan teknik serangan yang digunakan oleh perisian tersebut.

Mesin maya biasanya mengguna pakai teknologi seperti pemisahan mesin maya daripada sistem utama, pengesan tingkah laku, analisis keabadian, serta mekanisme kawalan dan pemulihan untuk memastikan keselamatan dan kestabilan sistem utama. Ia membantu dalam mengembangkan penyelesaian keselamatan yang lebih baik, mengesan dan menganalisis ancaman baru, serta memperoleh pemahaman yang lebih mendalam tentang perisian berbahaya.

Penggunaan mesin maya berguna dalam bidang keselamatan siber, penyelidikan perisian hasad, pengembangan perisian, serta analisis keselamatan. Ia membolehkan penyelidik dan pakar keselamatan siber untuk melaksanakan analisis mendalam dan menguji perisian dengan cara yang terkawal, menjadikannya alat penting dalam usaha melindungi sistem dan rangkaian daripada ancaman siber.

2.2.5 Kotak Pasir Perisian Hasad

Kotak pasir perisian hasad, juga dikenali sebagai “Malware Sandbox” dalam bahasa Inggeris, merujuk kepada persekitaran yang dikawal dan terasing yang digunakan untuk menjalankan dan menganalisis perisian hasad atau fail yang mencurigakan. Ia dirancang khusus untuk mengkaji tingkah laku perisian hasad tanpa mengancam keselamatan sistem utama.

Kotak pasir perisian hasad berfungsi sebagai lingkungan simulasi yang terasing dari sistem utama. Ia membolehkan penyelidik atau pakar keselamatan siber untuk menjalankan perisian hasad dalam persekitaran terkawal yang menghalang kesan negatif dan penyebaran perisian hasad ke luar kotak pasir. Ini memastikan keselamatan sistem sebenar dan melindungi maklumat sensitif daripada pengaruh yang berbahaya.

Apabila perisian hasad dijalankan dalam kotak pasir, aktivitinya dipantau dan dianalisis dengan teliti. Kotak pasir ini sering dilengkapi dengan mekanisme pemantauan tingkah laku, pengesan ancaman, serta rekod aktiviti yang mencurigakan.

Analisis yang dijalankan dalam kotak pasir membolehkan penyelidik memahami cara kerja perisian hasad, mengesan tindakan yang berpotensi merosakkan atau mencuri maklumat sensitif, dan mengenal pasti teknik serangan yang digunakan.

Penggunaan kotak pasir perisian hasad sangat penting dalam penyelidikan keselamatan siber, pengujian perisian, dan analisis ancaman. Ia membantu mengenal pasti dan memahami perisian hasad, memperbaiki mekanisme keselamatan, dan mengembangkan langkah-langkah perlindungan yang lebih baik terhadap serangan perisian hasad yang berbahaya.

Perbezaan diantara mesin maya dan kotak pasir ditunjukkan di Jadual 2.1:

Jadual 2.1 Perbandingan mesin maya dan kotak pasir

	Mesin Maya	**Kotak Pasir**
Tujuan	Merangkumi sistem pengendalian dan persekitaran perkakasan yang lengkap.	Mengasingkan dan melaksanakan fail yang berpotensi berniat jahat dalam persekitaran terkawal.
Persekitaran Pelaksanaan	Berjalan di atas sistem pengendalian hos	Berjalan dalam sistem operasi hos atau dalam persekitaran maya.
Pengasingan Sumber	Menyediakan pengasingan yang kuat antara sistem hos dan mesin maya.	Menyediakan pengasingan, tetapi mungkin mempunyai pemisahan yang kurang mantap berbanding mesin maya.
Pengekalan	Perubahan yang dibuat dalam mesin maya dipelihara sepanjang sesi.	Perubahan yang dibuat dalam kotak pasir biasanya dibuang selepas analisis.
Rangkaian	Boleh dikonfigurasikan untuk mempunyai sambungan rangkaian yang serupa dengan sistem hos.	Akses rangkaian boleh dihadkan atau dihadkan untuk menghalang perisian hasad daripada merebak.
Rintangan Pengesanan	Sesetengah perisian hasad boleh mengesan persekitaran maya dan mengubah tingkah lakunya.	Mungkin terdedah kepada perisian hasad yang lebih canggih yang dapat mengesan persekitaran kotak pasir.
Fleksibiliti Analisis	Membolehkan pemeriksaan mendalam dan di peringkat sistem pengendalian.	Memberikan keterlibatan terhad ke dalam sistem pengendalian yang mendasari tetapi memberi tumpuan kepada analisis tingkah laku.

bersambung…

...sambungan

Kesan Prestasi	Mungkin mempunyai keperluan sumber yang lebih tinggi dan boleh memberi kesan kepada prestasi sistem.	Biasanya mempunyai keperluan sumber yang lebih rendah dan kesan minimum terhadap prestasi sistem.
Interaksi Pengguna	Boleh menyediakan antara muka pengguna yang lengkap untuk berinteraksi dengan sistem maya.	Biasanya tidak mempunyai antara muka pengguna dan digunakan terutamanya untuk analisis automatik.

2.2.6 Kotak Pasir Perisian Hasad dalam Talian

Kotak pasir perisian hasad dalam talian, juga dikenali sebagai perkhidmatan kotak pasir perisian hasad dalam talian, merujuk kepada platform atau perkhidmatan yang menyediakan persekitaran simulasi terkawal secara dalam talian untuk menjalankan dan menganalisis perisian hasad atau fail mencurigakan. Ia membolehkan pengguna menguji perisian dalam persekitaran terkawal untuk memahami tingkah laku dan potensi ancaman yang mungkin dihadapi.

Beberapa nama popular untuk kotak pasir perisian hasad dalam talian adalah:

Any.Run: Merupakan perkhidmatan kotak pasir perisian hasad dalam talian yang popular. Ia membolehkan pengguna menjalankan perisian hasad secara langsung dalam persekitaran terkawal dan menganalisis kesan serta tingkah laku perisian tersebut.

Hybrid Analysis: Platform ini menyediakan kotak pasir perisian hasad dalam talian yang membolehkan pengguna menjalankan perisian hasad atau fail mencurigakan secara dalam talian. Ia menyediakan laporan dan analisis mendalam mengenai aktiviti perisian tersebut.

VirusTotal: Selain daripada perkhidmatan pengimbasan perisian hasad, VirusTotal juga menyediakan ciri kotak pasir perisian hasad dalam talian. Pengguna boleh menghantar fail mencurigakan untuk menjalankannya dalam persekitaran terkawal dan menganalisis tingkah laku serta potensi ancaman.

Joe Sandbox: Merupakan perkhidmatan kotak pasir perisian hasad dalam talian yang kuat dan sering digunakan dalam analisis perisian hasad. Ia menyediakan maklumat terperinci mengenai tindakan perisian hasad dan memberikan analisis yang komprehensif.

Cuckoo Sandbox: Platform ini menyediakan kotak pasir perisian hasad dalam talian yang boleh dihoskan secara sendiri. Ia membolehkan pengguna menjalankan perisian hasad dan menganalisisnya untuk mengenal pasti tingkah laku dan ancaman yang mungkin timbul.

2.2.7 Fuzzy Hashing

Fuzzy hashing adalah teknik dalam bidang keselamatan siber yang digunakan untuk mengesan kepelbagaian atau perbezaan di antara fail atau data. Ia melibatkan penggunaan fungsi hash untuk menghasilkan nilai yang unik untuk setiap fail atau data yang diberikan.

Apabila menggunakan fuzzy hashing, fungsi hash digunakan untuk mengira nilai hash bagi setiap blok data dalam fail. Keunikan teknik ini terletak pada keupayaannya untuk menghasilkan nilai hash yang hampir sama atau serupa untuk fail yang serupa, walaupun ada sedikit perbezaan di antara mereka. Dalam konteks keselamatan siber, teknik ini digunakan untuk mengesan perubahan yang berlaku dalam fail atau data yang mungkin disebabkan oleh perubahan kecil atau penyembunyian yang dilakukan oleh penyerang.

Fuzzy hashing berguna dalam pengesanan perisian hasad, analisis forensik digital, dan pengesanan serangan jaringan. Ia membolehkan penyelidik atau pakar keselamatan siber mengesan dan mengklasifikasikan fail atau data yang serupa atau berkaitan dengan kes sama ada dalam kes pengesanan perisian hasad atau dalam analisis forensik yang melibatkan perbandingan fail atau data yang disita.

Dengan menggunakan fuzzy hashing, dapat dikenal pasti keserupaan antara entiti yang berbeza dengan cepat dan berkesan. Ini membantu dalam pengenalpastian dan analisis ancaman dengan mengesan perubahan yang berlaku pada peringkat fail

atau data, dan membantu dalam mengambil langkah-langkah keselamatan yang sesuai untuk melindungi sistem dan maklumat sensitif.

2.2.8 Analisis Statik

Analisis statik perisian hasad merujuk kepada proses menganalisis perisian hasad tanpa menjalankannya secara aktif. Ia melibatkan pemeriksaan struktur, kod sumber, atau fail perisian untuk mengenal pasti tanda-tanda atau ciri-ciri yang mencurigakan yang mungkin menunjukkan kehadiran perisian hasad.

Kelebihan analisis statik perisian hasad adalah bahawa ia tidak melibatkan risiko menjalankan perisian secara langsung, membolehkan penyelidik atau pakar keselamatan siber menganalisis dan mengesan perisian hasad tanpa mengaktifkannya. Ini memberi keselamatan tambahan dan mengurangkan risiko sebarang kesan negatif pada sistem.

Namun, analisis statik perisian hasad juga mempunyai kelemahan, terutamanya dalam mengenal pasti perisian hasad yang telah disulitkan dengan teknik penyembunyian yang canggih. Perisian hasad yang menggunakan teknik penyulitan, pemulihan kod, atau pengaburan kod boleh sukar dikenal pasti melalui analisis statik sahaja.

Kombinasi analisis statik dengan analisis dinamik dan penggunaan alat-alat keselamatan siber lainnya adalah disyorkan untuk mendapatkan pemahaman yang lebih menyeluruh tentang perisian hasad dan memaksimumkan pengesanannya. Dengan memadukan pendekatan-pendekatan ini, penyelidik atau pakar keselamatan siber dapat mengesan perisian hasad dengan lebih berkesan dan mengambil tindakan yang sesuai untuk melindungi sistem daripada ancaman tersebut.

2.2.9 Analisis Dinamik

Analisis dinamik perisian hasad merujuk kepada proses menganalisis perisian hasad dengan menjalankannya secara aktif dalam persekitaran terkawal. Ia melibatkan

pengawasan dan pemantauan perisian hasad semasa ia berinteraksi dengan sistem untuk mengenal pasti tingkah laku dan kesan yang dihasilkan.

Dalam analisis dinamik, perisian hasad dijalankan dalam persekitaran kawalan yang sering disebut sebagai kotak pasir perisian hasad. Ketika perisian hasad beroperasi dalam kotak pasir, aktivitinya dipantau dan direkodkan dengan teliti. Persekitaran ini boleh mencatat arus kawalan, perubahan fail sistem, aktiviti rangkaian, serta interaksi dengan fail lain dan peranti keras.

Analisis dinamik perisian hasad membolehkan penyelidik atau pakar keselamatan siber untuk menganalisis secara terperinci tindakan dan kesan perisian hasad. Ini memungkinkan mereka untuk mengenal pasti tindakan yang mencurigakan, seperti perubahan terhadap fail sistem, cubaan mengakses sumber daya terlarang, penghijrahan ke sistem yang berbeza, atau penghantaran data yang tidak sah.

Kelebihan analisis dinamik adalah bahawa ia membolehkan pemantauan secara langsung terhadap perisian hasad semasa operasinya, memberikan pemahaman yang lebih mendalam tentang taktik, teknik, dan ancaman yang dihadapinya. Ia juga membolehkan pengesan perisian hasad yang menggunakan teknik evasi atau hanya beraktiviti pada keadaan tertentu.

Walau bagaimanapun, analisis dinamik mungkin melibatkan risiko yang lebih tinggi kerana perisian hasad sebenar dijalankan. Oleh itu, langkah-langkah keselamatan yang kukuh dan kaedah yang betul perlu diambil untuk melindungi sistem utama daripada risiko yang mungkin timbul semasa analisis.

Kombinasi analisis dinamik dengan analisis statik dan penggunaan alat-alat keselamatan siber lainnya adalah disyorkan untuk mendapatkan pemahaman menyeluruh tentang perisian hasad dan mengesan serta menghadapinya secara berkesan. Dengan menggunakan pendekatan gabungan ini, penyelidik atau pakar keselamatan siber dapat mengenal pasti dan menganalisis perisian hasad dengan lebih baik, dan mengambil tindakan yang sesuai untuk melindungi sistem daripada ancaman tersebut.

2.3 PENGGUNA AKHIR ADALAH TITIK LEMAH DALAM KESELAMATAN SIBER

Dalam kajian Tam et al. (2021), terdapat fokus pada kedudukan keselamatan siber dan penyelesaian yang berkaitan dengan perniagaan kecil dalam julat 0-19 pekerja yang sangat terhad, mengingat pentingnya perniagaan mikro/kecil dalam ekonomi global. Walaupun banyak kajian telah dilakukan mengenai keselamatan siber dalam perniagaan korporat besar dari pelbagai negara, aplikasi kajian tersebut ke dalam perniagaan kecil masih menjadi masalah yang belum teratasi. Dalam konteks ini, pengaruh faktor komunikasi dan manusia terhadap serangan seperti penipuan phishing dan penipuan melalui e-mel menjadi penting. Selain itu, faktor saiz juga menjadi pertimbangan penting dalam diskusi tentang keselamatan siber

Definisi standard untuk keselamatan siber belum ada, dan kebanyakan definisi yang ada hanya ditujukan kepada para profesional. Oleh kerana itu, memahami dan menjelaskan keselamatan siber kepada bukan pakar menjadi tantangan bagi pengamal dan peneliti. Ini berpotensi menghadapi kesulitan ketika berkomunikasi dengan pengguna awam, karyawan organisasi, dan perniagaan kecil yang kurang memiliki keahlian dalam IT atau tenaga kerja keamanan siber (Neil et al., 2023).

Keselamatan siber adalah penting untuk semua PKS, terutamanya semasa pandemik global Covid-19 yang mengancam ini. Peralihan secara tiba-tiba meninggalkan pejabat untuk bekerja dari rumah - 'normal baru' - telah memperkenalkan risiko berkaitan keselamatan maklumat yang berkaitan dengan faktor manusia. (Ncubukezit, 2022)

Komputer dan Keselamatan Maklumat (Computer and Information Security - CIS) biasanya didekati dengan sudut pandang yang tertumpu kepada teknologi, di mana komponen manusia dalam sistem sosioteknik umumnya dianggap sebagai bahagian yang paling lemah, dengan sedikit pertimbangan terhadap ciri-ciri kognitif, keperluan, dan motivasi pengguna akhir. (Pollini et al., 2021)

Kesilapan pekerja menimbulkan risiko dalam syarikat. Contohnya ialah apabila pengguna ingin tahu, melulu dan jahil membuka e-mel palsu yang mengandungi

lampiran perisian hasad yang dipasang secara automatik apabila dibuka. Selain itu, pengguna boleh memasang perisian hasad yang dilampirkan pada aplikasi standard. Selalunya pakej pemasangan yang dijangkiti boleh didapati di laman sesawang untuk memerangkap pengguna yang tidak dapat diketahui. (Ncubukezit, 2022)

Dalam kajian (Pollini et al., 2021), penulis telah menggunakan taksonomi kesilapan manusia dan rangka kerja pelanggaran seperti di Jadual 2.2:

Jadual 2.2 Taksonomi kesilapan dan pelanggaran manusia

Tindakan keselamatan yang salah	**Jenis ralat/pelanggaran**	**Keterangan**
Tindakan tidak sengaja dan tidak sengaja menentukan pelanggaran peraturan keselamatan	Tergelincir berasaskan kemahiran	Tindakan yang salah dalam tugas yang rutin dan hanya memerlukan pemeriksaan sedar sekali-sekala; Kesilapan ini berkaitan dengan perhatian individu yang melakukan tindakan yang relevan untuk keselamatan
	Kesilapan dalam kemahiran	Kegagalan ingatan dalam tindakan yang berkaitan dengan keselamatan, seperti meninggalkan tindakan yang dirancang atau melupakan niat keselamatan yang berkaitan
Tindakan sengaja menentukan pelanggaran peraturan keselamatan yang tidak diingini	Kesalahan berasaskan peraturan	Penggunaan peraturan buruk yang berkaitan dengan keselamatan. Penggunaan peraturan yang tidak sesuai yang relevan untuk keselamatan.
	Kesilapan berasaskan pengetahuan	Perbuatan yang disengajakan yang melibatkan pengetahuan konseptual yang salah, pengetahuan yang tidak lengkap, atau spesifikasi tindakan yang salah, yang membawa kepada pelanggaran dasar atau prosedur keselamatan yang tidak diingini.
Pelanggaran prosedur keselamatan yang disengajakan tanpa niat jahat	Pelanggaran	Sisihan yang disengajakan daripada dasar atau prosedur keselamatan kerana meremehkan akibat keselamatan (boleh menjadi rutin atau luar biasa)
Pelanggaran prosedur keselamatan yang disengajakan dengan niat jahat	Pelanggaran berniat jahat	Sisihan yang disengajakan daripada dasar atau prosedur keselamatan untuk tujuan mensabotaj sistem

Dalam kajian Desolda et al., 2021, mereka telah menggunakan senarai "Dirty Dozen" yang digariskan oleh Dupont, yang mengandungi dua belas kesilapan paling biasa dalam aktiviti penyelenggaraan disebabkan oleh faktor manusia tertentu. Senarai ini dianggap sebagai asas yang sah untuk siasatan dalam kajian keselamatan siber.

1. Kekurangan Komunikasi: orang yang tidak berkomunikasi antara satu sama lain dalam persekitaran kerja dan / atau dalam talian.

2. Berpuas hati: perasaan keyakinan diri yang boleh menyebabkan kurangnya kesedaran tentang potensi bahaya.

3. Kekurangan Pengetahuan: tidak mempunyai pengetahuan khusus dan pengalaman yang cukup yang boleh membawa kepada keputusan yang buruk.

4. Gangguan: apabila perhatian pengguna telah diambil dari tugas yang mereka perlu lakukan.

5. Kekurangan Kerja Berpasukan: tidak memberikan sokongan yang mencukupi terhadap sekumpulan orang, rakan sekerja, dll, yang bergantung pada sokongan ahli kumpulan lain.

6. Keletihan: ia adalah tindak balas fisiologi akibat daripada tempoh kerja dan tekanan yang berpanjangan.

7. Kekurangan Sumber: tidak mempunyai sumber yang mencukupi (contohnya, masa, alat, orang, dll.) untuk menyelesaikan tugas.

8. Tekanan: tekanan untuk memenuhi tarikh akhir mengganggu keupayaan kami untuk menyelesaikan tugas dengan betul.

9. Kekurangan Ketegasan: tidak dapat atau dibenarkan menyatakan kebimbangan atau idea.

10. Stres: tekanan akut dan kronik daripada bekerja untuk tempoh yang lama atau isu-isu lain yang menuntut seperti keluarga atau masalah kewangan.

11. Kurang Kesedaran: tidak menyedari apa yang berlaku di persekitaran (kerja atau dalam talian), selalunya membawa kepada pemotongan tidak sedarkan diri daripada apa yang dilakukan oleh orang lain.

12. Norma: amalan tempat kerja yang berkembang dari masa ke masa, yang kemudiannya boleh mempengaruhi tingkah laku lain.

Selain itu, kajian Nifakos et al., 2021 telah menyimpulkan bahawa, walaupun banyak profesional penjagaan kesihatan menyedari serangan phishing dan bertindak balas dengan sewajarnya, pendidikan berterusan diperlukan di seluruh spektrum keselamatan siber, dengan penekanan khusus di sekitar "kebocoran" (leakage) maklumat di media sosial.

Keselamatan maklumat adalah bahagian penting dalam organisasi segerak yang dipamerkan terutamanya melalui penyelesaian teknologi keselamatan siber, seperti “firewall”, perisian antivirus, sistem pengesanan pencerobohan, pusat operasi keselamatan dan sebagainya. Namun, faktor manusia masih belum diiktiraf sebagai elemen teras rantaian keselamatan siber seperti yang ditunjukkan oleh laporan insiden ancaman siber dan kekurangan garis panduan serta maklumat berterusan mengenai bahaya keselamatan. (Georgiadou et al., 2021)

2.4 CABARAN MEMBINA KOTAK PASIR PERISIAN HASAD SENDIRI

Berdasarkan temu bual yang dijalankan oleh Yong Wong et al., 2021, walaupun peserta menghargai fleksibiliti kotak pasir sumber terbuka, salah satu kritikan utama mereka adalah perlunya usaha yang besar untuk melakukan persediaan yang betul. Selain itu, 3 peserta menyebut bahawa proses persediaan memerlukan pemahaman teknikal yang mendalam tentang bagaimana kotak pasir berfungsi.

Kajian oleh Kamal et al. 2021 menunjukkan bahawa Kotak pasir Cuckoo, yang berasaskan sistem operasi Linux, rumit untuk dipasang dan dikonfigurasi oleh individu biasa dalam bidang ilmu komputer. Selain itu, kajian tersebut juga menyelidiki penggunaan persekitaran kotak pasir untuk menganalisis fail perisian tebusan, namun, proses pemasangan awal dan pemahaman laporan yang dihasilkan sering kali merupakan tugas yang sukar. Tambahan pula, informasi penting yang diperlukan untuk

mengesan perisian tebusan sukar ditemukan dalam laporan yang dihasilkan oleh persekitaran tersebut.

Penganalisis dapat membangun mesin maya dari awal dan memasang peralatan yang diperlukan, tetapi ini memerlukan masa yang banyak. Selain itu, semasa mengkonfigurasi peralatan, mudah terjadi kesalahan yang tidak disengajakan. Penganalisis juga biasanya memiliki waktu yang terbatas kerana tekanan untuk menyelesaikan masalah keamanan jaringan dengan cepat, yang memerlukan analisis, penilaian, dan penyelesaian yang segera dilakukan (Le et al., 2022).

Gibert et al., 2020 telah menunjukkan bahawa risiko menggunakan mesin maya dan penggunaan kotak pasir untuk analisis perisian hasad adalah bahawa sesetengah perisian hasad dapat mengesan apabila ia berjalan dalam mesin maya atau kotak pasir dan seterusnya, ia akan melaksanakan tindakan yang berbeza berbanding dengan apabila berjalan pada mesin fizikal, menjadikan tugas analis perisian hasad lebih sukar. Tambahan pula, walaupun pengguna mengambil semua langkah berjaga-jaga yang mungkin, risiko sentiasa wujud ketika menganalisis perisian hasad. Dari semasa ke semasa, kelemahan telah ditemui dalam alat mesin maya yang membenarkan pihak serang mengeksploitasi beberapa ciri-cirinya seperti ciri perkongsian folder.

2.5 MANFAAT MESIN MAYA DAN KOTAK PASIR PERISIAN HASAD DALAM TALIAN

Dalam temu bual oleh Yong Wong et al., 2021, didapati bahawa 7 peserta Tier 2 melengkapkan sampel mereka dengan perisian hasad tambahan yang ditemui di repositori seperti VirusTotal, Reversing Labs, Malware Bazaar, The Zoo, AnyRun, Malshare, Hybrid Analysis, Malpedia, dan Twitter. Amalan ini dilakukan untuk membolehkan analis mempunyai pelbagai sampel yang luas untuk dianalisis, dengan tujuan menghasilkan tandatangan yang mempunyai liputan yang lebih meluas.

Yong Wong et al., 2021 juga menunjukkan bahawa membezakan antara tingkah laku berbahaya dan tidak berbahaya dalam hasil analisis dinamik adalah tugas yang mencabar dalam amalan. Menurut peserta P6, untuk menggunakan kotak pasir, pengguna perlu memahami dengan baik tentang tingkah laku asas. Tidak cukup hanya

meletakkannya dalam kotak pasir dan menerima semua hasilnya. Pengguna perlu dapat membezakan dan mengenali tingkah laku yang normal untuk Windows dan Adobe. Ini adalah aspek yang sering menipu banyak orang.

Symantec menghindari jurang pelaporan sendiri ini dengan menggunakan perisian pengesanan ancaman yang diketahui yang dipasang dalam komputer pengguna akhir. Menghapuskan interaksi manusia meningkatkan ketepatan dengan merakam butiran kejadian secara automatik. Walau bagaimanapun, sifat milikan perisian ini dan pelaporan mengakibatkan hanya pelanggan dan peranti Symantec yang terlibat. Ini mengakibatkan kecenderungan terhadap orang yang bersedia (dan mampu) untuk membayar perkhidmatan Symantec. (Tam et al., 2021)

VirusTotal merupakan platform imbasan yang popular di antara yang lain. Di VirusTotal, pengguna boleh memuat naik fail untuk diperiksa oleh lebih daripada 70 pembekal antivirus (AV), bagi menentukan sama ada fail tersebut berbahaya atau tidak. Selepas imbasan fail, platform ini menyediakan hasil pengesanan keseluruhan dari semua enjin pengesanan yang digunakan. Oleh itu, platform ini tidak menentukan sama ada aplikasi itu berbahaya atau tidak; sebaliknya, ia bergantung kepada pengguna untuk menentukan strategi dalam menafsirkan maklumat yang disediakan. (Leka et al., 2022)

Untuk proses analisis berlaku dengan lebih cepat dan memanfaatkan alat sumber terbuka, kami mencadangkan proses analisis asas berdasarkan Fire Eye Ekosistem. Flare VM bertujuan untuk penganalisis profesional. Oleh itu, banyak alat berharga telah ditambah, terutamanya alat sumber terbuka Fire Eye. (Le et al., 2022)

Dalam kajian oleh Lee, 2023, ditemui bahawa teknik berdasarkan tandatangan biasanya digabungkan dengan analisis statik untuk mencari tandatangan khusus pada perisian hasad. Namun, pendekatan ini tidak dapat menangkap tandatangan unik yang hanya dihasilkan semasa pelaksanaan perisian hasad, seperti pakej rangkaian, panggilan API, urutan “opcode”, dan lain-lain. Analisis statik terhadap perisian hasad yang disulitkan adalah mustahil secara asas. Oleh itu, kumpulan ciri-ciri ini perlu dikombinasikan dengan pelaksanaan perisian hasad melalui implementasi kod hasad buatan dan/atau simulasi pengamat dalam persekitaran mesin maya yang terasing

sepenuhnya daripada rangkaian luar, seperti laman sesawang palsu. Inilah sebabnya ciri-ciri seperti ini dikenali sebagai ciri-ciri tingkah laku, dan teknik pengesanan berdasarkan ciri-ciri ini dikenali sebagai pengesanan berdasarkan tingkah laku.

A. Darem, 2022 telah mengkaji bahawa penyelesaian pengesanan perisian hasad konvensional bergantung kepada tandatangan yang diekstrak daripada contoh perisian hasad melalui kejuruteraan songsang perisian hasad. Pendekatan-pendekatan ini sudah tidak lagi berkesan kerana penulis perisian hasad secara berterusan mengubah tandatangan perisian hasad. Kompleksiti pengesanan perisian hasad juga meningkat dengan ketara dengan peningkatan jumlah perisian hasad pada kadar yang membimbangkan. Selain itu, penulis perisian hasad menggunakan pelbagai teknik untuk mengelakkan pengesanan.

Berdasarkan temu bual Yong Wong et al., 2021, mengenal pasti sama ada sampel adalah variasi daripada yang sebelumnya dianalisis adalah tugas biasa bagi kebanyakan analis perisian hasad untuk mengelakkan analisis yang berulang. Dalam temu bual tersebut, 14 peserta menyatakan bahawa proses ini masih merupakan cabaran. Sebagai contoh, peserta P2 menjelaskan bahawa tidak terdapat alat atau sumber yang baik, terutamanya yang percuma, untuk membantu dalam bidang tersebut.

Yong Wong et al., 2021 juga menyimpulkan bahawa menentukan kesamaan dua fungsi perisian hasad adalah salah satu tugas yang memerlukan masa yang lama menurut 8 peserta yang dikaji. Peserta P21 menyatakan bahawa mengidentifikasi kesamaan fungsi di antara dua perisian binari (binary) merupakan masalah yang sangat kompleks yang cuba diatasi sebaik mungkin. Menghasilkan hasil yang dapat dipercayai dan mencapai kesesuaian di antara kedua-duanya merupakan tantangan yang berat.

Selain itu, dalam kajian Aboaoja et al., 2023, mendapatkan set data yang mewakili merupakan tugas yang sukar kerana kebanyakan penyelidik tidak memberikan akses kepada set data mereka.

Dalam kajian oleh Lee, 2023, diketahui bahawa pengesanan berdasarkan tandatangan kerap digunakan dalam keselamatan maklumat tradisional untuk mengesan

perisian hasad dengan menggunakan tandatangan kod hasad yang diketahui. Analisis statik digunakan untuk mencari tandatangan unik pada kod hasad. Kaedah pengesanan berdasarkan tandatangan dapat mengesan aplikasi hasad yang diketahui dengan ketepatan tinggi. Namun, pengesanan kelemahan “zero-day” adalah mustahil kerana diperlukan tandatangan unik yang diketahui. Selain itu, penyerang boleh mengelakkan pengesanan dengan menggunakan teknik seperti pengaburan kod (code obfuscation) untuk menghalang penemuan tandatangan unik.

Dalam kajian Ahn et al., 2022, didapati bahawa sistem kawalan keselamatan yang sedia ada tidak dapat mengesan dan menganalisis perkembangan progresif kod hasad dengan berkesan. Ini menyebabkan peningkatan yang ketara dalam pengesanan positif palsu dan pengesanan negatif palsu, menjadikan tugas penilaian dan tindak balas oleh pentadbir menjadi sukar. Selain itu, teknologi analisis kod hasad statik tidak efektif dalam mengesan kod hasad yang tidak diketahui, manakala teknologi analisis kod hasad dinamik pula boleh mempunyai kelajuan yang terlalu perlahan.

2.6 PERBINCANGAN

Kajian ini mendapati bahawa membina kotak pasir perisian hasad sendiri adalah baik. Ia memberikan individu lebih banyak fleksibiliti untuk menguji fail yang tidak diketahui dengan cara mereka sendiri. Walau bagaimanapun, ini memerlukan pengetahuan teknikal pelbagai komponen, seperti mesin maya, konfigurasi rangkaian, dan sistem operasi. Tanpa pemahaman yang kukuh tentang konsep-konsep ini, sukar untuk mengkonfigurasi persekitaran kotak pasir dengan betul.

Keselamatan siber perniagaan kecil tidak boleh "cut and paste" dari penyelesaian berskala besar. Ketersediaan sumber, landskap teknikal, dan proses operasi perniagaan kecil memerlukan pertimbangan yang teliti. Keselamatan siber memerlukan analisis risiko dan pengurangan keseluruhan sistem IT, bukan hanya komponen individu. Belanjawan IT kecil perniagaan kecil tidak meliputi gaji pentadbir IT. Tambahan pula, pemilik perniagaan kecil berada dalam kelemahan pengetahuan dalam menyokong keperluan keselamatan siber mereka. (Tam et al., 2021)

Landskap teknikal perniagaan kecil berpotensi sangat berbeza dengan perniagaan korporat besar, menjadikan tidak praktikal untuk mengaplikasikan penyelesaian yang digunakan untuk pengguna berskala besar kepada pengguna berskala kecil. Landskap teknikal IT perniagaan kecil ("senibina") di mana penyelesaian keselamatan siber perlu berfungsi merupakan halangan untuk mengambil pendekatan penyelesaian tersebut. (Tam et al., 2021)

Walaupun kepentingan keselamatan siber sangat penting, tiada definisi piawai bagi istilah ini. Selain itu, kerana definisi sedia ada kebanyakannya ditujukan kepada pakar dengan kepakaran dalam keselamatan siber, terdapat sedikit pemahaman mengenai definisi yang paling berguna untuk menjelaskan keselamatan siber kepada bukan pakar (mereka yang tidak mempunyai kepakaran dalam keselamatan siber). Ini mungkin menimbulkan cabaran kepada pengamal keselamatan dan penyelidik apabila cuba berkomunikasi makna dan kepentingan keselamatan siber kepada bukan pakar, termasuk pengguna awam, pekerja organisasi, dan perniagaan kecil yang tidak mempunyai kakitangan teknologi maklumat (IT) atau keselamatan siber yang khusus. (Neil et al.,2023)

Kotak pasir perisian hasad selalunya memerlukan konfigurasi perkakasan dan perisian tertentu untuk beroperasi dengan berkesan. Pengguna mungkin perlu mempunyai akses kepada mesin berkuasa dengan sokongan virtualisasi dan keupayaan untuk memperuntukkan sumber yang mencukupi untuk menjalankan pelbagai mesin maya secara serentak.

Kotak pasir perisian hasad biasanya menggunakan sistem pengendalian yang berbeza untuk mengasingkan dan menganalisis sampel perisian hasad. Ini memerlukan pengguna mempunyai pemahaman asas tentang pelbagai sistem pengendalian, seperti Windows, Linux, atau MacOS, untuk menyediakan dan mengkonfigurasi persekitaran kotak pasir dengan betul.

Selain itu, menganalisis perisian hasad secara berkesan memerlukan pengetahuan tentang pelbagai teknik dan alat, seperti analisis statik, analisis dinamik, dan kejuruteraan terbalik. Tanpa pengalaman atau latihan terdahulu, sukar bagi

pengguna akhir untuk memahami cara mengekstrak maklumat yang bermakna daripada sampel perisian hasad.

Secara rumusnya, analisis perisian hasad adalah tugas yang mencabar. Ia biasanya merupakan langkah pertama yang perlu dilakukan dalam pelan tindak balas insiden perisian hasad. Proses ini memerlukan penganalisis untuk menyediakan laporan dengan tepat dan cepat untuk melaksanakan penyelesaian yang diperlukan seterusnya. (Le et al., 2022)

Memandangkan cabaran ini, secara amnya disyorkan untuk pengguna akhir dengan pengetahuan dan kemahiran keselamatan siber yang terhad menyediakan mesin maya yang lebih mesra pengguna. Menyediakan VM adalah tugas biasa, dan akibatnya, terdapat banyak tutorial, panduan, dan dokumentasi yang tersedia dalam talian. Sumber-sumber ini menyediakan arahan langkah demi langkah dan petua penyelesaian masalah, menjadikannya lebih mudah bagi pengguna untuk menubuhkan VM walaupun dengan pengetahuan yang terhad.

Di samping itu, banyak platform virtualisasi menawarkan imej VM yang telah dikonfigurasikan, sering dipanggil "peralatan," yang disertakan dengan sistem operasi dan perisian yang telah dipasang terlebih dahulu. Pengguna boleh memuat turun imej ini dan mengimportnya dengan cepat ke dalam perisian virtualisasi mereka, mengurangkan kerumitan proses persediaan.

Topik lain yang akan dibincangkan ialah analisis statik dan analisis dinamik memberikan perspektif yang berbeza mengenai perisian hasad. Dengan menggabungkan kedua-dua teknik, pengguna akhir boleh mendapatkan pemahaman yang lebih komprehensif tentang tingkah laku perisian hasad dan kesan yang berpotensi. Analisis statik memberi tumpuan kepada memeriksa kod dan ciri-ciri fail perisian hasad itu sendiri, sementara analisis dinamik memerhatikan tingkah laku perisian hasad dalam persekitaran terkawal.

Analisis statik yang dilakukan dalam mesin maya membolehkan pengguna akhir menganalisis sampel perisian hasad di luar talian, tanpa sebarang sambungan rangkaian.

Ini amat berguna apabila berurusan dengan sampel sensitif atau sulit yang mereka tidak mahu muat naik ke kotak pasir dalam talian. Pengguna akhir boleh melakukan pemeriksaan mendalam terhadap kod, tingkah laku dan ciri lain perisian hasad tanpa menghantar sampel di luar persekitaran terkawal.

Kotak pasir perisian hasad dalam talian seperti VirusTotal menyediakan keupayaan analisis dinamik dengan melaksanakan sampel perisian hasad dalam persekitaran dalam talian yang terkawal. Kotak pasir ini sering memanfaatkan pelbagai sistem pengendalian, aplikasi dan konfigurasi rangkaian, yang membolehkan pemerhatian yang lebih pelbagai terhadap tingkah laku perisian hasad. Mereka juga memberikan pandangan tambahan dengan membandingkan perisian hasad dengan tandatangan yang diketahui dan penunjuk kompromi.

Kotak pasir perisian hasad dalam talian seperti VirusTotal mengekalkan pangkalan data yang luas bagi sampel perisian hasad yang diketahui dan kecerdasan ancaman yang berkaitan. Dengan menghantar sampel ke platform ini, pengguna akhir boleh memanfaatkan repositori luas mereka untuk mengakses laporan, analisis tingkah laku, dan kadar pengesanan dari pelbagai enjin antivirus. Ini membantu pengguna akhir mendapatkan cerapan tentang kelaziman, status pengesanan perisian hasad dan tindak balas yang berpotensi.

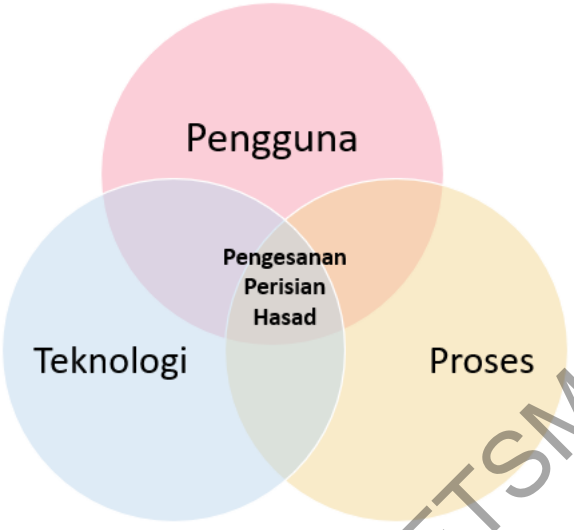
Ia dapat membantu perniagaan kecil dan sederhana (PKS) mengesan potensi perisian berbahaya atau fail yang mencurigakan sebelum menyebabkan kerosakan kepada sistem mereka. PKS boleh menggunakan VirusTotal untuk mendapatkan pandangan terperinci tentang status keselamatan fail dan URL, mengenal pasti positif palsu, dan membuat keputusan yang berinformasi mengenai ancaman yang mungkin. Tambahan pula, ia boleh menjadi berguna terutamanya bagi PKS dengan sumber yang terhad, kerana menyediakan cara yang berkos efektif untuk meningkatkan keupayaan pengesanan perisian berbahaya.

Pemetaan untuk penyataan masalah, soalan penyelidikan dan objektif penyelidikan, kaedah dan hasil dirumuskan di Jadual 2.3

Jadual 2.3 Jadual pemetaan untuk penyataan masalah, soalan penyelidikan, objektif penyelidikan dan hasil

Penyataan Masalah	**Soalan Penyelidikan**	**Objektif Penyelidikan**	**Kaedah**	**Hasil**
Pengguna akhir menimbulkan cabaran dalam mengendalikan perisian hasad, menjadikannya titik kelemahan dalam rantaian keselamatan. Tingkah laku pengguna akhir, termasuk kurang kesedaran, kelemahan terhadap taktik kejuruteraan sosial dan kesilapan, menyebabkan serangan perisian hasad terutamanya di PKS.	Apakah faktor yang mempengaruhi pengguna akhir terhadap kesediaan keselamatan siber?	Mengenal pasti faktor-faktor kesediaan keselamatan siber oleh pengguna akhir	Ulasan Kepustakaan	Rangka kerja konsep keselamatan siber (pengguna, proses, teknologi)
Kerumitan yang terlibat dalam menubuhkan kotak pasir perisian hasad memberikan halangan bagi pengguna akhir. Kerumitan ini menghalang keupayaan mereka menggunakan sistem kotak pasir dengan berkesan, dan mengehadkan keupayaan mereka untuk menganalisis potensi ancaman.	Bagaimanakah pengguna akhir boleh memanfaatkan mesin maya, kotak pasir perisian hasad dalam talian, fuzzy hashing untuk meningkatkan keberkesanan dan ketepatan pengesanan perisian hasad?	Membangunkan langkah asas untuk pengguna akhir berdasarkan rangka kerja keselamatan siber NIST	Eksperimen	Langkah-langkah khusus NIST untuk pengguna akhir dalam PKS

2.7 RANGKA KERJA KONSEP: PENGGUNA, PROSES, TEKNOLOGI (PPT) MODEL UNTUK PENGESANAN PERISIAN HASAD



Rajah 2.1 Rangka Kerja Konsep: Pengguna, Proses, Teknologi (PPT) model untuk pengesanan perisian hasad

Rangka Kerja Pengguna, Proses, Teknologi (PPT) adalah model yang digunakan secara meluas yang menekankan tiga komponen utama yang diperlukan untuk pelaksanaan dan pengurusan sistem atau inisiatif yang berjaya. Keselamatan siber juga memerlukan penyertaan pengguna, proses, dan teknologi dalam organisasi untuk melindungi organisasi, orang, dan infrastruktur IT secara kolektif daripada serangan siber. (Berlilana et al., 2021).

Oleh itu, model "Pengguna, Proses, Teknologi" ini menjadi inspirasi dalam penyelidikan ini, di mana penyelidikan ini akan mengadaptasi rangkaian konseptual tersebut yang disesuaikan untuk pengesanan perisian hasad. Rajah 2.1 menyesuaikan rangka kerja konsep "Pengguna, Proses, Teknologi" untuk pengesanan perisian hasad sambil mempertimbangkan konteks khusus pengguna akhir di PKS dengan pengetahuan dan bajet yang terhad dapat meningkatkan pertahanan keselamatan siber.

Apabila menggabungkan elemen "pengguna akhir", rangka kerja boleh diwakili seperti berikut: "Pengguna" mewakili pengguna akhir yang terlibat dalam sistem. "Proses" merujuk kepada ulasan kepustakaan yang dijalankan untuk memahami cabaran dihadapi oleh pengguna akhir sesama menyemak fail-fail yang tidak diketahui. Selain

itu, "Proses" juga dimaksudkan aliran kerja, prosedur dan metodologi rangka kerja keselamatan siber NIST yang digunakan untuk mencapai tugas dan mencapai matlamat untuk pengesanan perisian hasad. "Teknologi" mewakili alat, sistem, perisian, dan perkakasan yang digunakan untuk menyokong dan menyempurnakan proses. Teknologi adalah penggunaan mesin maya dan kotak pasir perisian hasad dalam talian.

2.7.1 Pengguna (Pengguna Akhir)

Dari segi kepakaran keselamatan siber, pengguna akhir yang bekerja di PKS biasanya boleh dikategorikan kepada tiga tahap yang luas:

Pengguna Asas / Umum (basic): Tahap ini termasuk kebanyakan pekerja yang menggunakan komputer dan sistem digital sebagai sebahagian daripada kerja mereka tetapi mungkin tidak mempunyai pengetahuan atau latihan keselamatan siber khusus. Pengguna ini mempunyai pemahaman asas tentang amalan keselamatan seperti menggunakan kata laluan yang kuat, tidak mengklik pautan atau lampiran yang mencurigakan, dan memastikan perisian dikemas kini. Mereka secara amnya menyedari risiko keselamatan tetapi mungkin memerlukan pendidikan dan peringatan berterusan untuk mengekalkan tabiat keselamatan siber yang baik.

Pengguna Pertengahan (intermediate): Tahap ini terdiri daripada pengguna yang mempunyai pemahaman yang lebih mendalam tentang keselamatan siber dan mempunyai pengetahuan di luar amalan keselamatan asas. Mereka mungkin telah menerima beberapa bentuk program latihan atau kesedaran mengenai topik seperti mengenal pasti percubaan pancingan data, mengamalkan penyemakan imbas yang selamat, dan mengenali potensi ancaman. Pengguna pertengahan juga mungkin mempunyai beberapa kebiasaan dengan alat keselamatan dan amalan yang berkaitan dengan peranan pekerjaan khusus mereka.

Pengguna Lanjutan / Juara Keselamatan (advanced): Tahap ini terdiri daripada individu yang mempunyai pengetahuan dan kemahiran lanjutan dalam keselamatan siber dan secara aktif menyumbang kepada usaha keselamatan organisasi. Pengguna ini mungkin telah menerima latihan khusus, pensijilan, atau mempunyai pengalaman kerja yang berkaitan dalam bidang seperti keselamatan rangkaian, tindak balas insiden,

pengurusan kerentanan, atau pengekodan selamat. Mereka sering memainkan peranan penting dalam melaksanakan langkah-langkah keselamatan, melakukan penilaian risiko, menjalankan audit keselamatan, dan membantu dalam aktiviti tindak balas insiden. Pengguna lanjutan juga boleh bertindak sebagai mentor atau jurulatih untuk pekerja lain dan memberi panduan mengenai amalan terbaik keselamatan.

PKS mungkin mempunyai kumpulan pekerja yang lebih kecil, dan individu boleh melaksanakan pelbagai peranan dalam organisasi. Walau bagaimanapun, tahap umum ini menyediakan rangka kerja untuk memahami pelbagai tahap pengetahuan dan kemahiran keselamatan siber di kalangan pengguna akhir dalam PKS.

2.7.2 Proses (Ulasan Kepustakaan dan Rangka Kerja Keselamatan Siber NIST)

Ulasan Kepustakaan: Menjalankan ulasan kepustakaan menyeluruh untuk mengumpulkan pandangan dan amalan terbaik yang berkaitan dengan pengesanan perisian hasad. Terokai sumber yang bereputasi seperti kertas penyelidikan, laporan industri, dan blog keselamatan siber. Kenal pasti trend biasa, ancaman baru muncul, dan teknik pengesanan yang berkesan. Ini akan membantu memaklumkan perkembangan proses pengesanan perisian hasad yang mantap.

Rangka Kerja Keselamatan Siber NIST: Manfaatkan Rangka Kerja Keselamatan Siber NIST sebagai panduan untuk membangun dan meningkatkan proses pengesanan perisian hasad organisasi. Selaraskan amalan organisasi dengan fungsi Kenal Pasti, Lindungi, Kesan, Respons dan Pulih. Fokus pada fungsi Lindungi dan Kesan untuk memastikan pertahanan yang kuat dan mengenal pasti ancaman perisian hasad yang berpotensi tepat pada masanya.

2.7.3 Teknologi (Mesin Maya, Kotak Pasir dalam talian)

Mesin Maya (VM) - Flare VM: Menggunakan Flare VM, mesin maya yang tersedia secara percuma yang dibangunkan oleh FireEye, direka khusus untuk analisis perisian hasad dan kejuruteraan terbalik. Dengan memanfaatkan Flare VM, pengguna akhir boleh memeriksa fail yang berpotensi berniat jahat dengan selamat dalam persekitaran terpencil dan terkawal. Ini membantu mengurangkan risiko menjangkiti sistem hos

sambil membolehkan pengguna mempelajari dan mendapatkan pandangan tentang tingkah laku perisian hasad.

Kotak Pasir Dalam Talian - VirusTotal: Menggabungkan VirusTotal, platform kotak pasir dalam talian, ke dalam proses pengesanan perisian hasad. VirusTotal membolehkan pengguna akhir memuat naik fail yang mencurigakan dan menganalisisnya oleh pelbagai enjin antivirus dan teknologi pengesanan lain. Ini menyediakan lapisan analisis tambahan dan meningkatkan kemungkinan mengenal pasti perisian hasad.

Dengan menyesuaikan rangka kerja "Pengguna, Proses, Teknologi" dengan fokus pada pengguna akhir, ulasan kepustakaan, Rangka Kerja Keselamatan Siber NIST, dan memanfaatkan alat seperti Flare VM dan VirusTotal, PKS dapat meningkatkan keupayaan pengesanan perisian hasad mereka dengan ketara. Pendekatan ini membantu menangani pengetahuan yang terhad dan kekangan belanjawan PKS sambil memberi kuasa kepada pengguna akhir untuk memainkan peranan aktif dalam mengesan dan mencegah insiden perisian hasad. Akhirnya, ia bertujuan untuk mengurangkan risiko menjadi mangsa serangan siber, menyedari bahawa manusia sering menjadi pautan lemah dalam keselamatan siber.

2.8 KESIMPULAN

Secara ringkas, terdapat kajian yang menunjukkan bahawa pengguna akhir adalah titik lemah dalam keselamatan siber dan membina kotak pasir perisian hasad sendiri memerlukan pengetahuan teknikal yang mendalam dan pemahaman tentang bagaimana kotak pasir perisian hasad berfungsi. Ini tidak sesuai untuk pengguna akhir yang hanya memiliki pengetahuan terhad. Banyak kotak pasir perisian hasad dibina dalam sistem operasi Linux sumber terbuka, ini menjadikan kebanyakan pengguna akhir sukar untuk menyediakan kotak pasir perisian hasad sendiri.

Kajian juga menunjukkan penggunaan kotak pasir perisian hasad sendiri juga melibatkan risiko tertentu kerana perisian hasad boleh memalsukan tingkah laku semasa pelaksanaannya. Selain itu, individu perlu mengemas kini dan mengemas kini alat-alat

di dalam kotak pasir perisian hasad secara berkala untuk mengelakkan penggunaan eksploitasi perisian hasad.

Oleh itu, kajian ini menggalakkan pengguna akhir untuk menggunakan mesin maya mudah dan kotak pasir perisian hasad dalam talian yang boleh didapati secara umum untuk menguji fail-fail yang tidak diketahui. Dengan melakukan kedua-dua kaedah ini, ia akan memastikan analisis statik dan analisis dinamik dijalankan untuk mengatasi kekurangan dalam pengesanan berdasarkan tandatangan.

BAB III

KAEDAH KAJIAN

3.1 PENGENALAN

Bab ini membincangkan kaedah kajian dan kesesuaian pemilihan tersebut di dalam keseluruhan penyelidikan bagi menjawab persoalan dan mencapai objektif kajian. Kaedah kajian yang akan diterangkan meliputi reka bentuk kajian, fasa kajian yang dilaksanakan serta kaedah dah teknik yang digunakan.

Projek yang bakal dijalankan adalah di bawah bidang keselamatan komputer dan rangkaian yang akan tertumpu kepada analisis perisian hasad. Projek ini adalah bersifat pengguna akhir mempergunakan mesin maya yang tidak memerlukan teknikal ilmu yang ketara, dan menggunakan kotak pasir perisian hasad dalam talian untuk mengetengahkan pendekatan analisis statik dan dinamik. Sebagai langkah keselamatan, projek ini hanya akan mendapatkan contoh perisian hasad daripada sumber yang dipercayai.

Projek ini akan mengguna perisian mesin maya popular VirtualBox dengan memuat turun sistem operasi ISO Windows 10 versi penilaian 90 hari bertujuan penilaian. Projek menggunakan Flare VM yang telah dikonfigurasi khusus dalam lingkungan Windows. untuk keperluan analisis perisian hasad dan penentuan keselamatan digital. Di samping itu, projek akan menggunakan kotak pasir perisian hasad dalam talian VirusTotal untuk mendapatkan informasi komprehensif dan pemahaman yang lebih baik tentang perisian hasad.

Pemilihan Flare VM dan VirusTotal disebabkan oleh banyaknya alat analisis perisian hasad yang tersedia di platform Windows dan kebanyakan alatan adalah percuma untuk digunakan.

3.2 REKA BENTUK KAJIAN

Dalam kajian ini, penyelidikan empirikal akan digunakan. Creswell & Creswell, 2018 menyatakan dalam penyelidikan empirikal, prosesnya biasanya bermula dengan rumusan soalan penyelidikan atau hipotesis. Ini berfungsi sebagai titik permulaan bagi kajian dan memandu keseluruhan proses penyelidikan. Penerokaan susastera bertujuan untuk mendapatkan latar belakang dan maklumat mengenai bidang yang dikaji melalui penelitian hasil kajian terdahulu. Teknik yang digunakan semasa aktiviti ini ialah analisis kandungan terhadap artikel, kertas pembentangan, kertas persidangan, buku, dan juga dokumen terbitan Kerajaan.

Setelah soalan penyelidikan ditetapkan, penyelidik meneruskan dengan pengumpulan data. Ini boleh melibatkan pelbagai kaedah seperti eksperimen, pemerhatian, tinjauan, temu bual, atau penyelidikan arkib. Data yang dikumpulkan adalah berdasarkan pemerhatian atau pengalaman dunia sebenar. Dalam kajian ini, eksperimen dan pemerhatian akan digunakan.

Setelah data dikumpulkan, ia akan melalui proses analisis. Bergantung kepada sifat penyelidikan, kaedah analisis kuantitatif atau kualitatif boleh digunakan. Analisis kuantitatif melibatkan kaedah statistik untuk mengkaji data berangka, manakala analisis kualitatif melibatkan pengekodan, pengkategorian, dan interpretasi data teks atau pemerhatian.

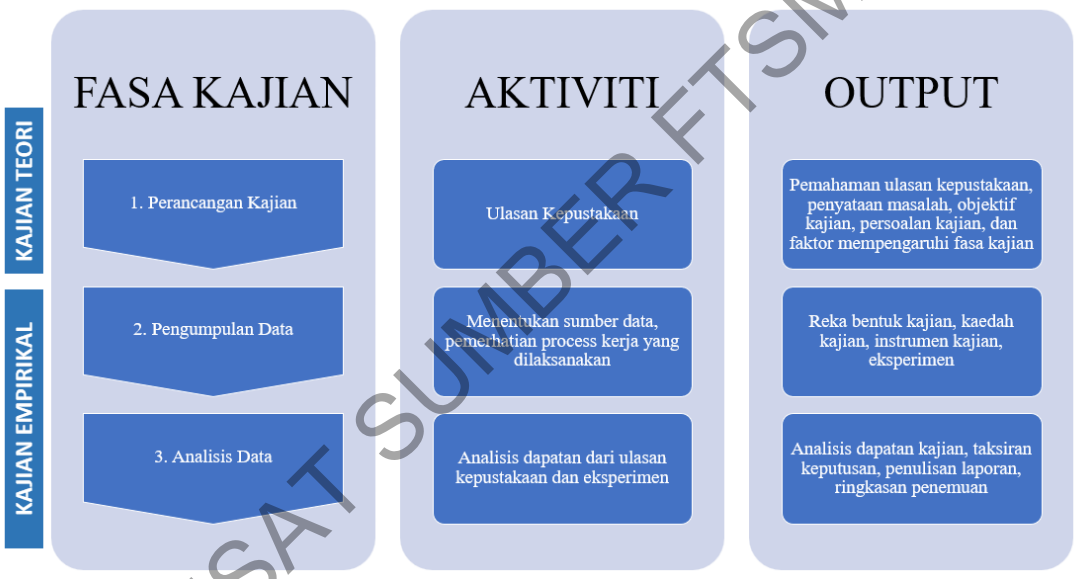
Dalam kes menggunakan VirusTotal, penyelidik boleh mengumpul data kuantitatif mengenai pengesanan perisian hasad dan melakukan analisis statistik mengenai hasilnya. Ini termasuk mengukur kadar kejayaan pengesanan perisian hasad, menganalisis kadar positif palsu atau negatif palsu, dan membandingkan prestasi kaedah pengesanan yang berbeza. Selain itu, pengguna akhir digalakkan menggunakan mesin maya - Flare VM untuk menguji fail perisian hasad dan mendokumentasikan tingkah laku mereka biasanya akan berada di bawah penyelidikan kualitatif.

Hasil yang diperoleh daripada fasa analisis data kemudian diinterpretasikan dan dibincangkan berdasarkan soalan penyelidikan atau hipotesis. Ini melibatkan

menghubungkan hasil dengan teori-teori sedia ada, memberikan penjelasan atau wawasan, serta mengenal pasti corak atau hubungan dalam data.

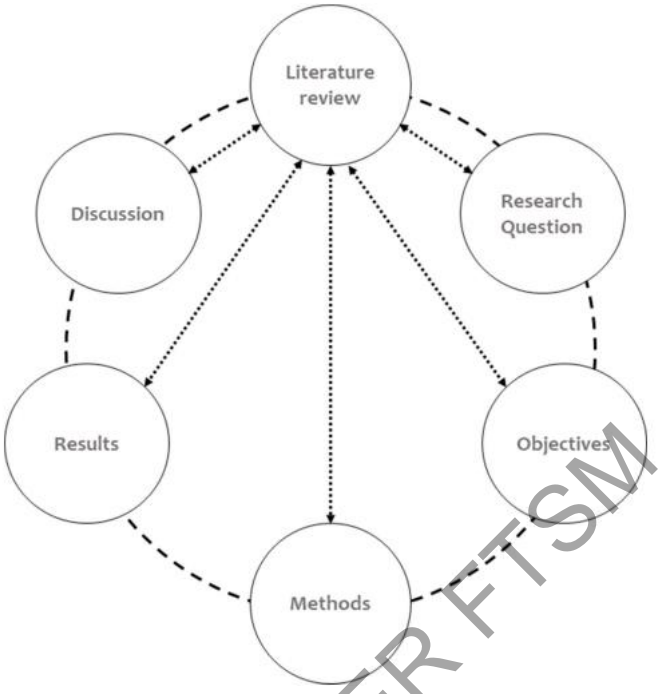
Akhirnya, penyelidik menyediakan kesimpulan berdasarkan hasil dan interpretasi tersebut. Kesimpulan ini akan menjawab soalan penyelidikan atau hipotesis dan mungkin juga merangkumi implikasi, batasan, dan cadangan untuk penyelidikan lanjut.

Reka bentuk kajian ini telah diringkaskan di dalam Rajah 3.1



Rajah 3.1 Reka bentuk kajian

3.3 KAEDAH ULASAN KEPUSTAKAAN



Rajah 3.2 Unsur-unsur penting dalam Ulasan Kepustakaan

Sumber: (Leite et al., 2019)

Bab Ulasan Kepustakaan adalah komponen unsur tesis dan disertasi, dan ia disambungkan terus ke bahagian lain. Dengan menilai bab Ulasan Kepustakaan, pembaca akan menjangkakan apa yang diharapkan dari bahagian teks akademik yang tinggal. (Leite et al., 2019). Rajah 3.2 telah menunjukkan unsur-unsur penting dalam ulasan kepustakaan.

Di dalam ulasan kepustakaan ini, langkah-langkah penting penulisan ulasan kepustakaan yang diilhamkan oleh (Winchester & Salji, 2016). Ia dirumuskan di dalam Rajah 3.3.

Rajah 3.3 Langkah-langkah penting penulisan ulasan kepustakaan

Sumber: (Winchester & Salji, 2016)

Sumber-sumber kajian adalah diambil daripada artikel, jurnal, laman sesawang, laporan dalam tempoh masa 5 tahun (2019 hingga 2023). Jurnal-jurnal yang dikaji boleh didapati melalui Repositori Pembelajaran dan Penyelidikan UKM eResources@ptsl, UKM Journal Article Repository, E-THESIS FTSM UKM, Google Scholar, IEEE Xplore Digital Library, ScienceDirect, SpringerLink, Scopus, dan lain-lain.

Berikut adalah kata kunci utama yang dikenal pasti berkaitan dengan soalan penyelidikan:

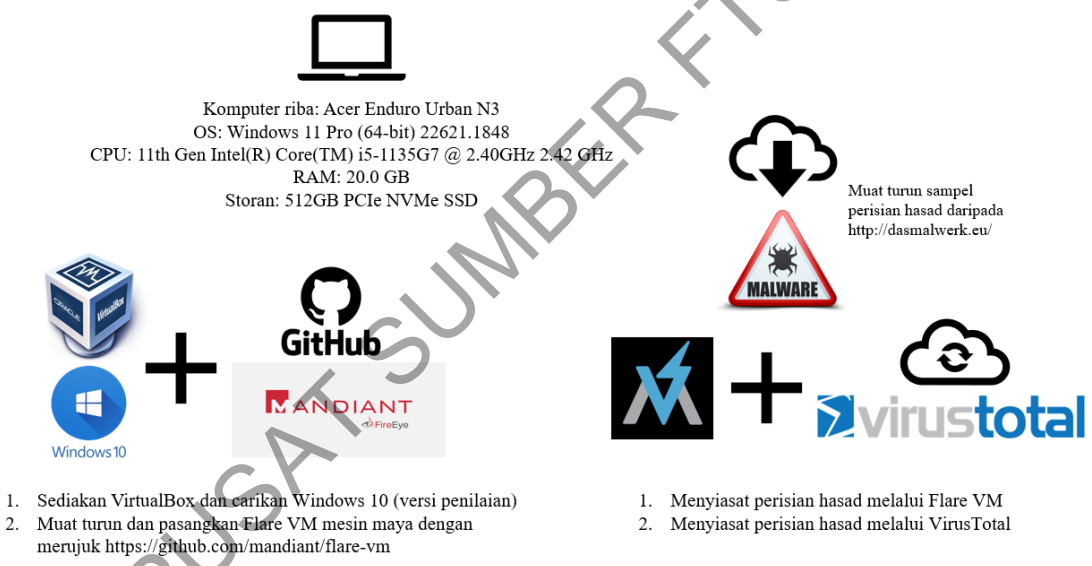
1. Challenge to setup malware sandbox **AND** difficult **AND** problem **AND** issue
2. End User is weakest link in cybersecurity **AND** human **AND** user
3. Limitation of static malware analysis **AND** challenge **AND** disadvantage **AND** problem **AND** issue **AND** barrier **AND** disadvantage **AND** obstacle
4. Cybersecurity readiness in SME **AND** human **AND** end user

Semua kata kunci dicari dalam bahasa Inggeris. Hasil carian lebih fokus kepada "Teks Penuh" dan “Jurnal Akademik”. Banyak artikel kini diterbitkan dengan akses terbuka dan boleh didapati terus dari laman sesawang jurnal secara percuma. Ini sangat berguna kerana seseorang dapat dengan cepat menentukan sama ada kertas itu menarik atau berkaitan dengan tinjauan kesusasteraan.

Pengendali Boolean “DAN” digunakan untuk mengurangkan jumlah hasil carian. Contoh hasil carian Repositori Pembelajaran dan Penyelidikan UKM eResources@ptsl telah ditunjukkan dalam Lampiran A.

3.4 INSTRUMEN KAJIAN

Eksperimen ini akan melibatkan penyediaan persekitaran mesin maya (Flare VM) yang mampu melaksanakan sampel perisian hasad secara asas. Tingkah laku sampel ini akan dipantau dan direkodkan dalam kotak pasir perisian hasad dalam talian (VirusTotal). Algoritma Fuzzy hashing akan dilaksanakan untuk membandingkan dan mengesan persamaan antara artifak memori yang dikumpulkan dan sampel perisian hasad.



Rajah 3.4 Reka Bentuk eksperimen secara ringkas

Rajah 3.4 menunjukkan penyediaan eksperimen untuk kajian ini. Dalam eksperimen ini, satu komputer riba akan digunakan. Sediakan versi penilaian Windows 10 dalam format VirtualBox, dan kemudian muat turun dan pasang Flare VM. Selepas itu, muat turun fail perisian hasad dari sumber yang tersedia secara awam. Eksperimen ini akan menggunakan Flare VM untuk analisis statik dan VirusTotal untuk analisis statik dan dinamik.

3.4.1 Perisian Virtualisasi – VirtualBox

VirtualBox adalah perisian yang membolehkan pengguna untuk menjalankan mesin maya atau sistem operasi maya di dalam komputer mereka. Ia adalah satu perisian hipervisor (hypervisor) yang membolehkan virtualisasi, iaitu mencipta persekitaran maya yang berasingan dan berbeza dari sistem operasi utama.

Dengan menggunakan VirtualBox, pengguna dapat memasang dan menjalankan sistem operasi tambahan di dalam mesin maya yang dibuat. Ini bermakna pengguna dapat menjalankan beberapa sistem operasi seperti Windows, Linux, atau MacOS di dalam komputer utama mereka, tanpa perlu memasangnya secara fizikal pada peranti keras yang berasingan.

VirtualBox menyediakan persekitaran terkawal yang membolehkan pengguna menguji aplikasi, mengembangkan perisian, dan menjalankan sistem operasi tambahan secara selari. Ia juga membolehkan pengguna untuk mengkonfigurasi sumber daya sistem seperti jumlah memori, ruang storan, dan peranti input-output untuk setiap mesin maya yang dijalankan.

Selain itu, VirtualBox juga menyediakan sokongan untuk kongsi papan kekunci dan tetikus antara sistem operasi maya dan sistem operasi utama, memudahkan pengguna untuk berinteraksi dengan kedua-dua persekitaran secara serentak.

VirtualBox merupakan perisian sumber terbuka yang dibangunkan oleh Oracle Corporation. Ia tersedia secara percuma untuk kegunaan peribadi dan komersial. Dengan fleksibiliti dan kebolehpercayaan yang ditawarkannya, VirtualBox telah menjadi salah satu pilihan yang popular bagi mereka yang ingin menjalankan mesin maya atau menjalankan sistem operasi tambahan di dalam komputer mereka.

Dalam kajian ini, versi Penilaian Windows 10 boleh didapati dari pautan ini https://archive.org/details/msedge.win10.virtualbox (Microsoft, 2018). Satu tangkapan skrin telah disediakan dalam Lampiran B.

Selain itu, langkah-langkah untuk memuat turun dan konfigurasi untuk VirtualBox versi 7.0.8 r156879 (Hos Windows) telah disediakan dalam Lampiran C.

3.4.2 Mesin Maya – Flare VM

Flare VM adalah sebuah alat atau perangkat lunak yang dibangunkan oleh FireEye, syarikat keselamatan siber terkemuka. Ia dirancang khusus sebagai satu-satunya mesin digital forensik dan alat analisis perisian hasad yang dihadapi oleh pakar penyiasat serta pengurus rangkaian. Flare VM menyediakan persekitaran yang disusun dengan baik yang membolehkan penyiasatan keselamatan siber dan analisis perisian hasad yang berkesan.

Flare VM berdasarkan sistem operasi Windows dan disusun dengan beberapa alat terkenal untuk memudahkan penyiasatan dan analisis. Antara alat yang termasuk adalah “debugger”, analisis perisian hasad, alat pemulihan, dan banyak lagi. Ia juga dilengkapi dengan pelbagai skrip dan utiliti tambahan yang disediakan oleh FireEye dan komuniti keselamatan siber untuk membantu dalam penyelidikan keselamatan siber dan analisis ancaman.

Kelebihan Flare VM termasuk kemudahan penggunaan, kelengkapan alat-alat penyiasatan dan analisis yang disediakan, serta kemampuan untuk berintegrasi dengan alat dan teknologi lain dalam persekitaran keselamatan siber. Ia juga terus dikemaskini dan diperbaharui oleh FireEye untuk mengatasi ancaman terkini dan memenuhi keperluan penyiasatan keselamatan siber yang semakin berkembang.

Flare VM sering digunakan oleh pakar keselamatan siber, penyiasat forensik, dan profesional IT yang terlibat dalam penyelidikan ancaman, analisis perisian hasad, atau pemulihan selepas serangan. Ia memberikan persekitaran yang terkawal dan siap sedia untuk menganalisis, mengesan, dan bertindak balas terhadap aktiviti berbahaya dalam sesebuah sistem komputer atau rangkaian.

Flare VM juga boleh disediakan secara manual dari awal. Langkah-langkah dan arahan boleh dirujuk di laman sesawang: https://github.com/mandiant/flare-vm (Updates, 2021) dan https://github.com/mandiant/flare-vm/blob/main/README.md

(Flare-Vm/README.md at Main · Mandiant/Flare-Vm, n.d.) Satu contoh tangkapan skrin Flare VM telah ditunjukkan dalam Lampiran D.

Dalam kajian ini, versi penilaian Windows 10 akan digunakan. Sebagai contohnya, pautan berikut mengandungi Flare VM pra-binaan dalam versi penilaian Windows 10. https://samsclass.info/126/Sum21/FLARE060721.7z (Samsclass.info: Sam Bowne Class Information, n.d.). Satu contoh tangkapan skrin Flare VM telah ditunjukkan dalam Lampiran E.

Semua alatan yang disediakan di dalam Flare VM telah dilampirkan seperti di Lampiran F. Penerangan mengenai setiap alatan boleh dirujuk melalui laman sesawang https://community.chocolatey.org/packages/ (Packages, n.d.)

Untuk Kajian ini, beberapa alatan berikut yang dipakai secara khusus (Jadual 3.1). Terdapat beberapa alat (CFF Explorer, die, exeinfope, peid, PE-bear, peview) yang digunakan untuk memeriksa dengan cepat fail-fail yang tidak diketahui untuk menentukan sama ada ia adalah fail PE atau fail “executable”. Setelah mengenal pasti bahawa fail tersebut adalah fail PE, kita boleh mengaktifkan beberapa alat pemantauan (proexp, ProcessHacker, autoruns, procmon) dalam Flare VM sebelum melaksanakan fail tersebut. Setelah siap, alat-alat pemantauan tersebut akan membantu kita memahami dengan lebih baik fail yang tidak diketahui semasa pelaksanaannya.

Jadual 3.1 Jadual mengenai alatan Flare VM yang digunakan

Alatan	**Penerangan**
CFF Explorer	Alat direka untuk memudahkan penyuntingan PE, tanpa kehilangan penglihatan pada struktur dalaman boleh laku mudah alih. Aplikasi ini merangkumi satu siri alat yang mungkin membantu jurutera terbalik (reverse engineering) dan pengaturcaraan.
die	Detect It Easy, atau disingkatkan DIE ialah program untuk menentukan jenis fail.
exeinfope	Exeinfo PE, ialah program untuk menentukan jenis fail.
sysinternals - autoruns	sysinternals mengandungi alat yang dipanggil Autoruns - ia adalah untuk memeriksa program apa yang dikonfigurasikan untuk permulaan secara automatik

bersambung...

...sambungan

peid	Alat untuk mengesan pembungkus (packers), cryptors dan pengkompil (compiler) yang digabungkan dengan PE boleh laku dengan bantuan perisian yang boleh dipercayai ini yang mempunyai kadar pengesanan yang tinggi
PE-bear	Pemapar fail/editor PE untuk analisis perisian hasad.
peview	Alat untuk melihat maklumat mengenai modul format boleh laku PE
ProcessHacker	Alat untuk melihat dan mengurus proses, perkhidmatan dan banyak lagi (alternatif untuk TaskMgr)
procexp	Alat menunjukkan maklumat tentang pengendalian dan proses DLL yang telah dibuka atau dimuatkan.
procmon	Alat pemantauan lanjutan untuk Windows

Satu lagi perkara yang perlu diberi perhatian ialah Flare-VM dengan v3.0.1 dikeluarkan pada April 30, 2021, telah menyokong Windows 10 x64, yang tidak disokong dalam versi terdahulu. Ia adalah perlu untuk konteks sokongan untuk Windows 7 tamat pada 14 Januari 2020. Satu lagi kelebihan Flare-VM adalah keserasian dengan hipervisor yang berbeza seperti VirtualBox, Qemu-KVM, VMware. (Le et al., 2022)

a. Langkah untuk menyediakan Flare VM

Panduan penuh boleh didapati melalui https://www.mandiant.com/resources/blog/flare-vm-update

1. Keperluan Sistem: Pastikan komputer memenuhi keperluan sistem minimum untuk menjalankan mesin maya. Flare VM adalah berdasarkan sistem pengendalian Windows, jadi pastikan sistem hos serasi.

2. Perisian virtualisasi: Pasang perisian virtualisasi seperti Oracle VM VirtualBox atau VMware Workstation Player pada sistem hos. Pakej perisian ini menjalankan mesin maya.

3. Muat turun Flare VM: Lawati repositori rasmi Flare VM GitHub di https://github.com/fireeye/flare-vm. Klik pada butang "Kod" dan pilih "Muat turun ZIP" untuk memuat turun pakej Flare VM sebagai arkib ZIP.

4. Ekstrak Flare VM: Cari arkib ZIP yang dimuat turun pada komputer dan ekstrak kandungannya ke lokasi pilihan. Ini akan mencipta folder yang mengandungi fail Flare VM.

5. Import Flare VM: Buka perisian virtualisasi (contohnya, VirtualBox atau VMware). Dalam antara muka perisian, cari pilihan untuk mengimport atau membuat mesin maya baru. Pilih pilihan untuk mengimport mesin maya sedia ada atau buat yang baharu menggunakan fail cakera keras maya (VHD) atau Format Virtualisasi Terbuka (OVF) sedia ada. Semak imbas ke folder di mana lokasi mengekstrak fail Flare VM dan pilih fail yang sesuai (contohnya, OVF atau VHD) untuk diimport.

6. Konfigurasikan Mesin Maya: Ikut gesaan pada skrin untuk mengkonfigurasi tetapan mesin maya. Sebagai contohnya, memperuntukkan sumber seperti CPU, memori, dan ruang storan untuk mesin maya. Sesuaikan sebarang tetapan tambahan berdasarkan keutamaan atau keperluan sistem. Keperluan minimum dan proses pemasangan daripada Flare-VM pada komputer Windows OS adalah storan cakera keras 60GB (hard drive storage) dan RAM 2GB (RAM) . Selepas proses pemasangan adalah lengkap, kita perlu mengambil “snapshot” untuk menyimpan status mesin untuk analisis berulang.

7. Mulakan Flare VM: Setelah mesin maya diimport dan dikonfigurasi, pilih mesin maya dari senarai dalam perisian virtualisasi. Klik pada butang "Mula" atau "Main" untuk melancarkan Flare VM.

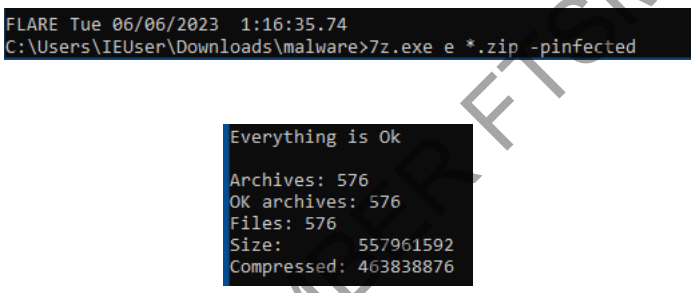
8. Sediakan Flare VM: Ikut arahan pada skrin dalam Flare VM untuk menyediakan konfigurasi dan keutamaan yang diperlukan. Ini mungkin melibatkan membuat akaun pengguna, memilih tetapan rangkaian, dan memasang sebarang kemas kini yang diperlukan atau perisian tambahan.

9. Mula menggunakan Flare VM: Setelah persediaan awal selesai, pengguna boleh mula menggunakan Flare VM untuk analisis perisian hasad dan tujuan kejuruteraan terbalik. Membiasakan diri dengan alat dan keupayaan yang ditawarkan oleh Flare VM dengan merujuk kepada dokumentasi dan panduan yang disediakan dalam pakej Flare VM.

Ingat untuk sentiasa mengemas kini Flare VM dan alat yang disertakan untuk memastikan versi terkini dan ciri keselamatan yang dikemas kini.

3.4.3 Set Data Perisian Hasad

Navigasi ke laman sesawang http://dasmalwerk.eu/ yang dimiliki oleh Robert Svensson, beliau adalah penyelidik terkenal dan pengarang buku untuk "*From Hacking to Report Writing*" (** Dasmalwerk.eu **, n.d.). Satu tangkapan skrin laman sesawang telah ditunjukkan dalam Lampiran G. Memuat turun sampel perisian hasad dan unzip semua ke dalam mesin maya Flare VM:



Rajah 3.5 Muat turun 576 perisian hasad

Berdasarkan laman sesawang pengarang, terdapat 623 sampel perisian hasad. Sebanyak 576 boleh dimuat turun (Rajah 3.5). Bakinya 47 tidak dapat dimuat turun.

3.4.4 Kotak Pasir Perisian Hasad dalam Talian - VirusTotal

VirusTotal adalah sebuah perkhidmatan dalam talian yang menyediakan pemeriksaan menyeluruh dan percuma terhadap fail dan URL (laman sesawang) untuk mengesan jangkitan perisian hasad atau ancaman keselamatan. Ia menggabungkan beberapa enjin antivirus dan alat-alat keselamatan lain untuk menganalisis dan mengesan kandungan berbahaya. Terdapat satu contoh tangkapan skrin laman sesawang VirusTotal telah ditunjukkan dalam Lampiran H.

Pengguna boleh menghantar fail atau URL ke laman sesawang VirusTotal, dan perkhidmatan ini akan mengimbasnya menggunakan pelbagai enjin antivirus dan alat keselamatan dari pelbagai pembekal. Hasil penyiasatan memberikan maklumat tentang

sama ada fail atau URL yang dihantar disahkan sebagai berbahaya atau mencurigakan oleh mana-mana pengimbasan tersebut.

VirusTotal juga menawarkan ciri-ciri tambahan seperti kemampuan untuk menganalisis proses yang sedang berjalan, memeriksa metadata fail yang terbenam, dan memeriksa fail berdasarkan senarai putih yang diketahui. Ia merupakan sumber unik yang membolehkan pengguna menilai risiko yang mungkin berkaitan dengan fail atau laman sesawang tertentu dengan cepat.

Perkhidmatan ini digunakan secara meluas oleh individu, organisasi, dan profesional keselamatan siber untuk melengkapkan langkah-langkah keselamatan mereka dan mendapatkan pandangan terhadap ancaman yang mungkin. Ia dapat membantu mengenal pasti dan meredakan perisian hasad, virus, trojan, cacing, dan jenis kandungan berbahaya lain yang mungkin membahayakan sistem komputer atau rangkaian.

a. Langkah untuk mendaftar VirusTotal

1. Lawati laman web VirusTotal: Pergi ke laman web rasmi VirusTotal di www.virustotal.com menggunakan penyemak imbas web.

2. Klik pada "Log masuk" atau "Buat Akaun": Di laman utama VirusTotal, cari butang "Log masuk" atau "Buat Akaun" dan klik padanya.

3. Pilih Kaedah Pendaftaran: VirusTotal menawarkan beberapa kaedah pendaftaran. Sebagai contoh, log masuk menggunakan akaun Google, Microsoft atau LinkedIn sedia ada atau mencipta akaun VirusTotal baharu. Pilih pilihan yang paling sesuai.

a. Akaun Sedia Ada: Jika pengguna memilih untuk log masuk menggunakan akaun sedia ada, ikut gesaan untuk membenarkan VirusTotal mengakses maklumat akaun.

b. Buat Akaun Baharu: Jika pengguna lebih suka membuat akaun VirusTotal baharu, pilih pilihan yang berkaitan dan berikan maklumat yang diperlukan,

seperti alamat e-mel dan kata laluan. Ikut gesaan untuk melengkapkan proses pendaftaran.

4. Sahkan E-mel (jika diperlukan): Bergantung pada kaedah pendaftaran pilihan pengguna, VirusTotal memerlukan pengesahan e-mel. Jika ya, semak peti masuk e-mel untuk e-mel pengesahan daripada VirusTotal. Buka e-mel dan klik pada pautan yang disediakan untuk mengesahkan alamat e-mel.

5. Log masuk ke VirusTotal: Setelah pendaftaran selesai dan pengesahan e-mel yang diperlukan dilakukan, kembali ke laman web VirusTotal. Klik pada "Log masuk" dan masukkan kelayakan akaun (alamat e-mel dan kata laluan) untuk log masuk.

6. Terima Syarat Perkhidmatan: Setelah log masuk buat kali pertama, pengguna digesa untuk menerima Syarat Perkhidmatan VirusTotal. Baca terma dan, jika bersetuju, klik pada kotak pilihan atau butang "Terima" untuk meneruskan.

7. Akses Ciri-ciri VirusTotal: Selepas berjaya mendaftar dan log masuk ke VirusTotal, pengguna akan mempunyai akses kepada pelbagai ciri seperti memuat naik fail untuk analisis, mencari laporan sedia ada, melihat hasil analisis dari pelbagai enjin antivirus, dan menggunakan fungsi tambahan yang disediakan oleh VirusTotal.

Nota: Sesetengah ciri VirusTotal memerlukan langganan premium, yang mungkin melibatkan langkah tambahan dan pembayaran. Walau bagaimanapun, analisis dan pelaporan perisian hasad asas biasanya boleh dilakukan dengan versi percuma VirusTotal.

Ingat untuk menggunakan VirusTotal secara bertanggungjawab dan mematuhi sebarang garis panduan dan dasar penggunaan yang ditetapkan oleh perkhidmatan.

b. Langkah untuk memuat naik fail yang tidak diketahui ke VirusTotal

1. Lawati laman web VirusTotal: Pergi ke www.virustotal.com menggunakan penyemak imbas web.

2. Log masuk ke akaun VirusTotal: Klik pada butang "Log masuk" yang terletak di laman utama VirusTotal. Masukkan kelayakan akaun (alamat e-mel dan kata laluan) untuk log masuk.

3. Navigasi ke halaman Muat Naik Fail: Setelah log masuk, pengguna akan diarahkan ke papan pemuka VirusTotal. Pada menu navigasi atas, klik pada "Fail" atau "Fail" untuk mengakses halaman muat naik fail.

4. Pilih fail untuk dimuat naik: Pada halaman muat naik fail, klik pada butang "Pilih Fail" atau "Pilih Fail". Ini akan membuka tetingkap pelayar fail pada komputer.

5. Pilih fail yang tidak diketahui: Dalam tetingkap penyemak imbas fail, cari dan pilih fail tidak diketahui yang mahu muat naik untuk semakan. Klik "Buka" atau "Pilih" untuk mengesahkan pilihan pengguna.

6. Muat naik fail: Selepas memilih fail, proses muat naik akan bermula secara automatik. Fail akan dipindahkan dengan selamat ke pelayan VirusTotal untuk analisis. Masa yang diperlukan untuk melengkapkan muat naik dan analisis bergantung pada saiz fail dan beban kerja semasa pada platform VirusTotal.

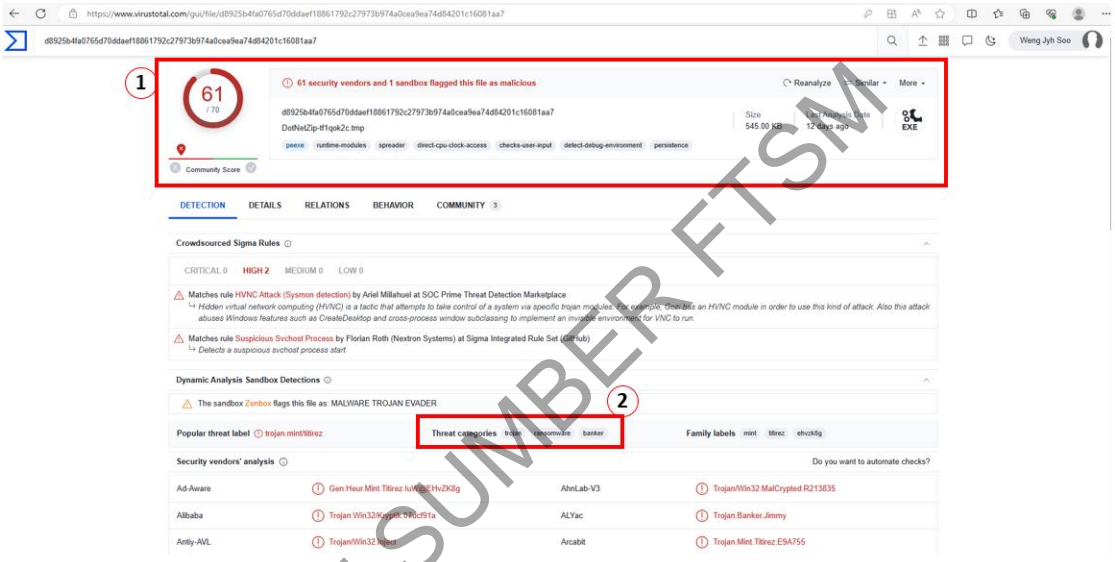
7. Lihat laporan analisis: Setelah fail dimuat naik dan dianalisis oleh VirusTotal, pengguna akan diarahkan ke halaman laporan analisis. Laporan ini memberikan maklumat terperinci tentang fail, termasuk hasil daripada pelbagai enjin antivirus dan alat keselamatan lain.

8. Mentafsirkan keputusan analisis: Pada halaman laporan analisis, semak hasil imbasan untuk melihat sama ada mana-mana enjin atau alat antivirus telah menandakan fail itu sebagai berniat jahat atau mencurigakan. Perhatikan nisbah pengesanan dan sebarang petunjuk khusus potensi ancaman.

9. Terokai ciri tambahan: VirusTotal menawarkan ciri dan fungsi tambahan untuk menyiasat lebih lanjut fail yang dimuat naik. Pengguna boleh mengakses ciri seperti analisis tingkah laku, laporan sejarah, komen komuniti dan banyak lagi untuk mendapatkan pandangan yang lebih mendalam tentang tingkah laku dan reputasi fail.

10. Ambil tindakan yang sesuai: Berdasarkan keputusan analisis, menilai tahap risiko fail dan tentukan tindakan yang sesuai untuk diambil. Jika fail dibenderakan sebagai berniat jahat, ambil langkah untuk kuarantin atau keluarkannya daripada sistem pengguna. Jika pengguna tidak pasti tentang keselamatan fail, berunding dengan pasukan IT atau keselamatan organisasi pengguna untuk panduan lanjut.

c. Cara-cara membaca dapatan VirusTotal

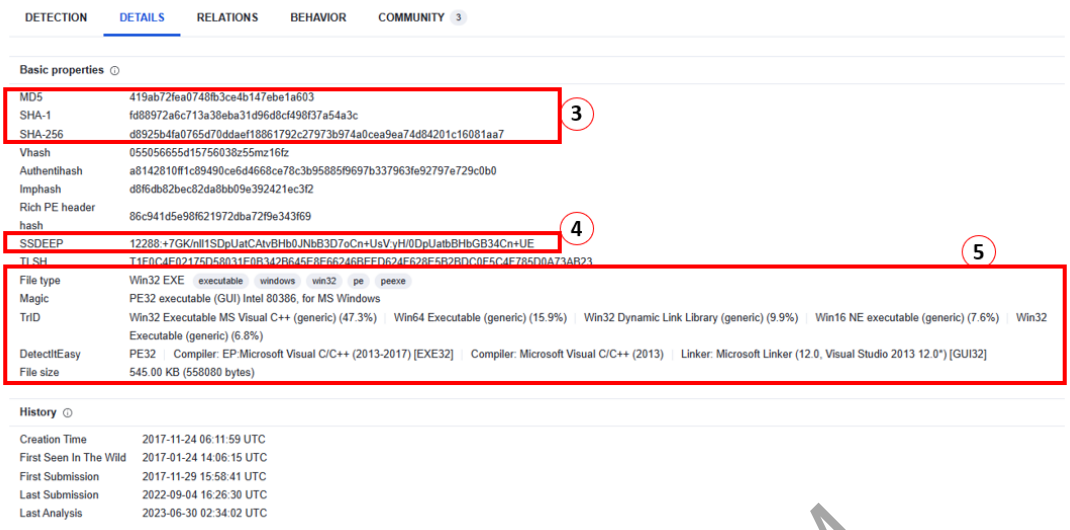


Rajah 3.6 Dapatan VirusTotal – Kiraan pengesanan perisian hasad dan kategori ancaman

Rajah 3.6 menunjukkan dapatan VirusTotal untuk kiraan pengesanan perisian hasad dan kategori ancaman.

1. Kiraan pengesanan perisian hasad: Jumlah rakan kongsi VirusTotal yang menganggap fail ini berbahaya (dalam kes ini, 61) daripada jumlah rakan kongsi yang menyemak fail (dalam kes ini, 70).

2. Kategori Ancaman: Kategori ancaman ini membantu mengelaskan dan memberikan gambaran keseluruhan potensi risiko atau tingkah laku berniat jahat yang berkaitan dengan fail.



Rajah 3.7 Dapatan VirusTotal – fungsi hash kriptografi dan analisis atribut fail

Rajah 3.7 menunjukkan dapatan VirusTotal untuk fungsi hash kriptografi dan analisis atribut fail.

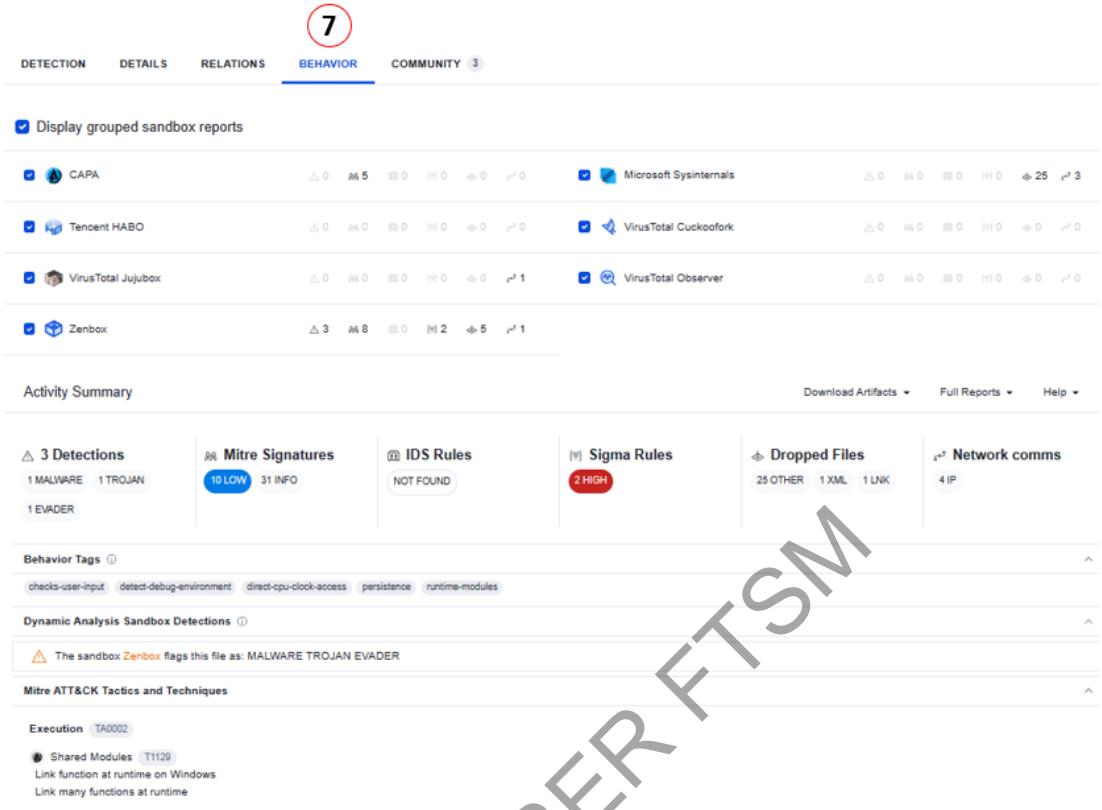
3. MD5, SHA1, SHA256: (fungsi hash kriptografi) adalah cara unik untuk mengenal pasti fail dan digunakan dalam industri keselamatan untuk merujuk secara jelas kepada ancaman tertentu

4. Nilai hash SSDEEP: fungsi hash kriptografi yang digunakan untuk mengira dan mewakili persamaan antara dua fail. Ia sering digunakan untuk mengenal pasti fail yang mempunyai kandungan yang serupa, walaupun mereka mempunyai nama yang berbeza atau sedikit pengubahsuaian.

5. Atribut Fail: Analisis atribut fail ini membantu dalam memahami jenis, format, saiz, pembungkus berpotensi yang digunakan dan ciri-ciri fail, membantu dalam analisis potensi ancaman atau fail yang mencurigakan.

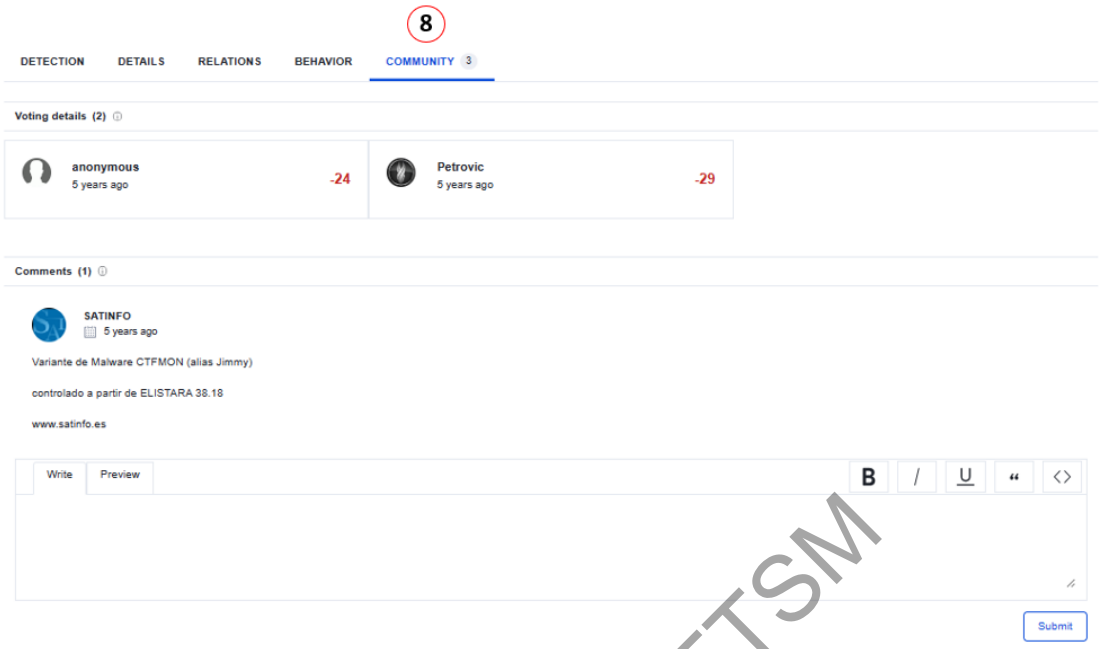
Rajah 3.8 Dapatan VirusTotal – hubungan antara elemen lain

6. Hubungan "Relations" tab dalam versi web dalam talian VirusTotal menyediakan maklumat mengenai hubungan dan hubungan antara pelbagai elemen, seperti fail, URL, domain, alamat IP dan banyak lagi. Ia membolehkan pengguna meneroka maklumat kontekstual dan persatuan yang berkaitan dengan item tertentu. (Rajah 3.8)



Rajah 3.9 Dapatan VirusTotal - analisis tingkah laku

7. Kelakuan “Behavior” tab memaparkan ringkasan tindakan yang dilakukan oleh item yang dianalisis dalam persekitaran terkawal atau memberikan akses kepada laporan analisis tingkah laku yang lebih terperinci. Maklumat ini (Rajah 3.9) dapat membantu penganalisis keselamatan dan penyelidik memahami potensi kesan dan tingkah laku fail atau URL, terutamanya apabila teknik analisis statik tradisional mungkin tidak mendedahkan sepenuhnya niat jahatnya.



Rajah 3.10 Dapatan VirusTotal – Komuniti

8. Komuniti "Community" tab: VirusTotal adalah ekosistem di mana semua orang menyumbang dan semua orang mendapat manfaat. Untuk mempromosikan kerjasama seperti ini, VirusTotal telah mencipta Komuniti VirusTotal (Rajah 3.10): ruang di mana industri antivirus, profesional keselamatan dan penyelidik perisian hasad boleh bercakap antara satu sama lain dan dengan pengguna akhir kerana kita semua berusaha untuk menjadikan internet tempat yang lebih selamat. Komuniti ini kini bertindak sebagai kecerdasan kolektif VirusTotal; Komen terdiri daripada analisis perisian hasad yang mendalam kepada maklumat mengenai vektor pengedaran dan lokasi dalam liar fail yang diserahkan. Fail dan URL boleh diundi sebagai berniat jahat atau tidak berbahaya; bersama-sama undi ini membina skor niat jahat komuniti untuk sumber.

3.4.5 Fuzzy Hashing - SSDEEP

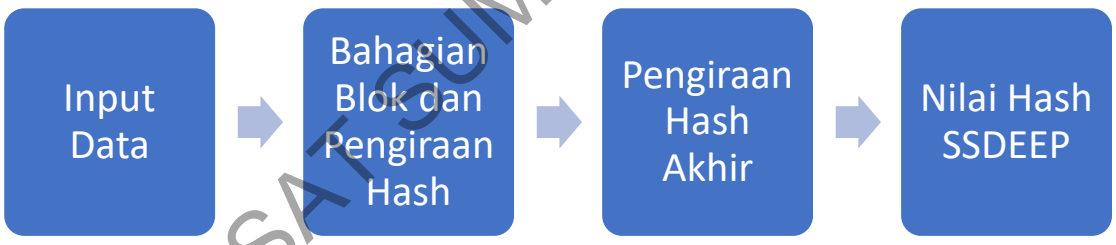
Fuzzy Hashing, juga dikenali sebagai hashing persamaan, menawarkan pendekatan unik untuk mengesan variasi dan persamaan dalam data. Dalam konteks pengesanan perisian hasad, fuzzy hashing boleh membandingkan dan mengenal pasti persamaan antara sampel perisian hasad, walaupun mereka mengalami sedikit pengubahsuaian atau

bersifat polimorfik. Dengan menjana nilai hash padat yang mewakili persamaan antara fail, hashing kabur membolehkan pengenalpastian varian perisian hasad yang berkaitan.

SSDEEP ialah algoritma fuzzy hashing yang mengira nilai hash untuk input tertentu, biasanya fail atau blok data. SSDEEP direka terutamanya untuk membandingkan dan mengenal pasti persamaan dalam kandungan fail.

SSDEEP berfungsi dengan membahagikan data input kepada blok saiz tetap, biasanya 64 bait. Ia kemudian menjana nilai hash bagi setiap blok berdasarkan kandungan blok tersebut. Nilai hash ini digabungkan untuk mewujudkan perwakilan hash akhir keseluruhan input.

Rajah 3.11 berikut adalah gambar rajah ringkas yang menerangkan langkah-langkah asas SSDEEP:



Rajah 3.11 Langkah-langkah asas SSDEEP

Dalam pembahagian blok dan langkah pengiraan hash, data input dibahagikan kepada blok saiz tetap. Bagi setiap blok, nilai hash dikira berdasarkan kandungan blok tersebut. Algoritma hashing khusus yang digunakan mungkin berbeza-beza, tetapi ia biasanya melibatkan teknik seperti cincangan atau fungsi hash kriptografi.

Tandatangan fuzzy hashing terdiri daripada dua bahagian yang dipisahkan oleh kolon. Bahagian pertama sebelum kolon mewakili saiz blok yang digunakan dalam algoritma fuzzy hashing. Nilai ini menunjukkan saiz blok yang fail dibahagikan kepada semasa proses hashing.

Bahagian kedua selepas kolon mewakili nilai hash sebenar, yang menangkap persamaan antara fail. Bahagian inilah yang digunakan untuk membandingkan dan memadankan fuzzy hashing antara satu sama lain untuk analisis persamaan.

Sebagai contoh, jika tandatangan fuzzy hashing ialah "192:AtWn7fBuXMYS11t7E7Ca9lnd6hQJhkT7PZwNUdQ", saiz blok yang digunakan untuk hashing ialah 192. Ini bermakna fail itu dibahagikan kepada blok 192 bait semasa proses fuzzy hashing.

Dalam langkah pengiraan hash akhir, nilai hash dari langkah sebelumnya digabungkan untuk mewujudkan perwakilan hash akhir keseluruhan input. Proses gabungan ini melibatkan pelbagai operasi seperti gabungan, peralihan bit dan operasi XOR untuk menjana perwakilan input yang padat dan unik.

Nilai hash ssdeep yang terhasil mewakili kandungan data input dan boleh digunakan untuk perbandingan dengan cincangan ssdeep lain untuk menentukan persamaan antara input yang berbeza.

3.4.6 Proses analisis perisian hasad

Kajian ini akan menjalankan proses analisis perisian hasad asas dengan menggunakan Flare VM dan VirusTotal. Ini adalah analisis terpilih yang mampu untuk pengguna akhir. Ini bukan senarai penuh semua alat yang disediakan dalam Flare VM dan VirusTotal.

Rajah 3.12 Proses analisis perisian hasad asas menggunakan Flare VM dan VirusTotal

Dalam kajian ini, terdapat beberapa jenis analisis yang boleh dicapai seperti ditunjukkan di Rajah 3.12, antaranya:

1. Analisis Atribut Fail: Analisis ini melibatkan pemeriksaan atribut fail seperti saiz fail, jenis fail, capaian masa, dan tandatangan digital. Ia membantu dalam memahami ciri-ciri fail yang dianalisis.
2. Analisis Pengepakan (Pack): Analisis pengepakan melibatkan pengesanan dan analisis fail yang telah dikepak atau diubahsuai secara tersembunyi. Ia membantu dalam membuka kepekatan fail untuk mendedahkan kod asal dan mengenal pasti tingkah laku yang mungkin berbahaya.
3. Analisis Rentetan (String): Analisis rentetan berfokus pada pengekstrakan dan analisis rentetan dalam fail. Ia membantu mengenal pasti pola atau petunjuk mencurigakan seperti URL, alamat IP, atau indikator kompromi lainnya.
4. Analisis Fungsi dan Metadata: Analisis fungsi dan metadata melibatkan pemeriksaan fungsi dan metadata dalam fail. Ia membantu dalam memahami tujuan, tingkah laku, dan ketergantungan fail tersebut.
5. Analisis Hash: Analisis hash dilakukan dengan membandingkan nilai hash fail dengan hash perisian berbahaya yang diketahui dalam pangkalan data VirusTotal. Ia membantu mengenal pasti perisian berbahaya yang telah diketahui berdasarkan tandatangan hashnya.

6. Analisis Keluarga Perisian Berbahaya: VirusTotal menyediakan maklumat mengenai keluarga perisian berbahaya atau sampel perisian berbahaya yang berkaitan. Analisis ini membantu dalam memahami konteks yang lebih luas mengenai ancaman yang dikenal pasti.
7. Analisis Tingkah Laku: VirusTotal mungkin menyediakan laporan analisis tingkah laku untuk beberapa fail, yang menunjukkan tingkah laku yang diperhatikan semasa pelaksanaan dalam persekitaran yang terkawal. Ia membantu mengenal pasti aktiviti yang mungkin berbahaya oleh fail tersebut.

Analisis-analisis disenaraikan di atas, bersama dengan Flare VM yang menyediakan persekitaran dan alat khusus untuk memudahkan teknik-teknik analisis serta sumbangan daripada platform VirusTotal telah menyediakan pelbagai enjin antivirus, membantu dalam mengesan dan mengenal pasti ancaman potensi, mengategorikan fail, serta memberikan pemahaman mengenai status keselamatan fail dan URL.

3.5 KESIMPULAN

Bab ini telah membincangkan kaedah dan pendekatan yang digunakan dalam penyelidikan ini. Kaedah ini merangkumi penggunaan ulasan kepustakaan untuk memahami landskap pengetahuan semasa dan asas teori yang berkaitan dengan topik kajian. Untuk melaksanakan eksperimen, kaedah, instrumen dan prosedur disediakan untuk menjalankan analisis data dan mengumpulkan bukti empirikal. Kaedah eksperimen ini telah dirancang untuk memeriksa aspek tertentu yang berkaitan dengan tajuk penyelidikan dan membantu dalam mencapai matlamat kajian secara berkesan. Penyelidikan ini berusaha untuk memberikan maklumat dan analisis yang mendalam tentang topik kajian, memberikan sumbangan yang signifikan kepada ilmu pengetahuan, dan menjawab dengan tepat soalan-soalan penyelidikan yang telah ditetapkan.

BAB IV

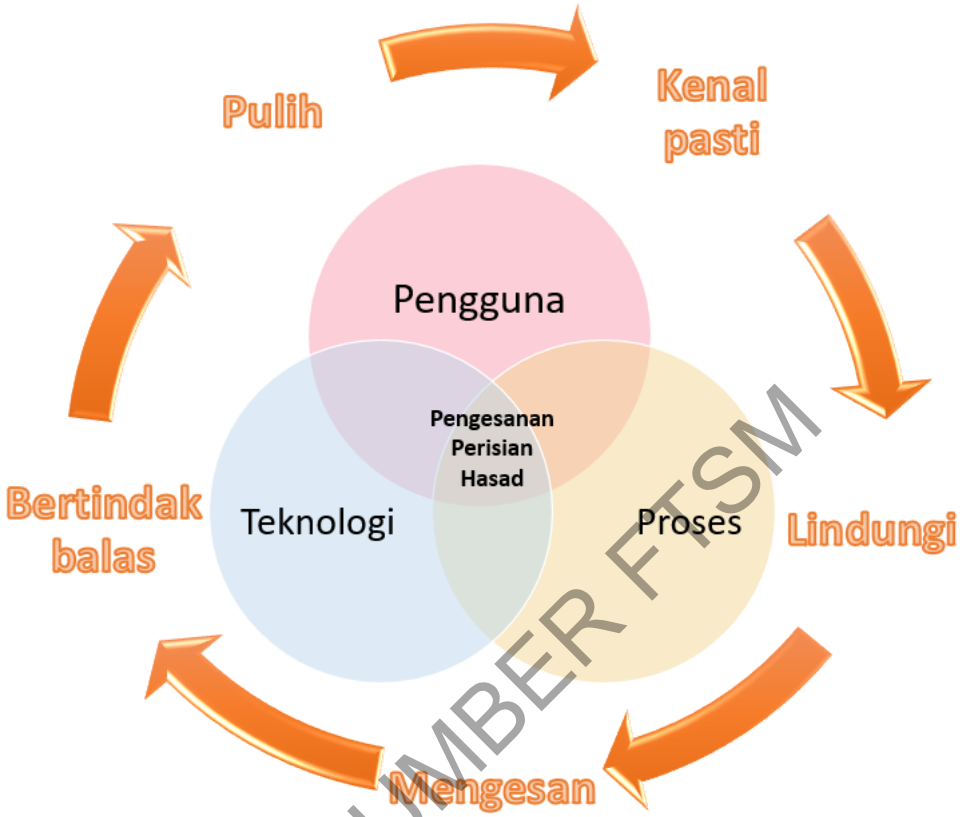
LANGKAH-LANGKAH DICADANGKAN KEPADA PENGGUNA AKHIR

4.1 PENGENALAN

Bab ini menerangkan kajian untuk mencadangkan penggabungan model "Pengguna, Proses, Teknologi" (People, Process, Technology) dengan rangka kerja keselamatan siber NIST.

Model "Pengguna, Proses, Teknologi" merangkumi tiga aspek utama untuk meningkatkan keselamatan siber dalam persekitaran perniagaan, khususnya dalam PKS. Dengan menggabungkan Rangka Kerja Keselamatan Siber NIST yang mengandungi lima komponen – "Kenal pasti, Lindungi, Mengesan, Bertidak Balas, Pulih" (Identify, Protect, Detect, Respond, and Recover), kajian ini dapat memahami bagaimana model ini mempengaruhi perspektif manusia sebagai pengguna akhir dalam PKS. Langkah-langkah dan prosedur yang dicadangkan harus mudah diikuti oleh pengguna akhir dan tidak membebankan PKS dalam adaptasinya.

4.2 HUBUNGAN ANTARA MODEL "PENGGUNA, PROSES, TEKNOLOGI" DAN RANGKA KERJA KESELAMATAN SIBER NIST



Rajah 4.1 Hubungan antara model “Pengguna, Proses, Teknologi” dan Rangka Kerja keselamatan Siber NIST

Rajah 4.1 di atas menunjukkan hubungan antara model “Pengguna, Proses, Teknologi” dan Rangka Kerja keselamatan Siber NIST. Penerangan untuk keperluan kajian ini adalah seperti berikut:

1. Pengguna (People):

Pengguna akhir, terutamanya yang bekerja dalam PKS, memegang peranan penting dalam keselamatan siber. Mereka perlu didedahkan kepada latihan kesedaran siber yang berkala untuk memahami ancaman siber semasa dan cara mengenal pasti tanda-tanda potensi perisian hasad atau serangan lain. Kesedaran terhadap kepentingan keselamatan siber harus menjadi kebiasaan harian bagi pengguna akhir. Rangka kerja NIST yang pertama, Kenal pasti (Identify) menekankan pengenalan dan pemahaman mengenai risiko dan potensi ancaman. Oleh itu, melalui pendekatan ini, pengguna akhir

dalam PKS akan lebih peka terhadap potensi ancaman siber dan berperanan sebagai barisan pertahanan pertama dalam mengenal pasti dan melaporkan sebarang kejadian mencurigakan.

2. Proses (Process):

Prosedur yang dicadangkan harus dirancang dengan teliti untuk memastikan kesederhanaan dan keberkesanannya dalam persekitaran PKS. Proses-proses ini harus mudah diimplementasikan dan tidak memerlukan tahap pengetahuan teknikal yang tinggi daripada pengguna akhir. Sebagai contoh, dalam model ini, setelah fail dikaji menggunakan VirusTotal, apabila jumlah pengesanan melebihi 10, langkah selanjutnya adalah melaporkan kepada jabatan IT atau pasukan keselamatan. Proses ini harus mudah dan dapat dilaksanakan oleh pengguna akhir tanpa menjejaskan operasi harian PKS. Rangka kerja NIST berikutnya, Lindungi (Protect) menitikberatkan perlindungan terhadap sistem dan data dari ancaman siber, dan prosedur yang mudah diikuti ini akan membantu PKS memenuhi matlamat perlindungan ini dengan lebih baik.

3. Teknologi (Technology):

Penggunaan teknologi yang tepat dan mesra pengguna sangat penting dalam mengekalkan keselamatan siber dalam PKS. Apabila menggunakan alat seperti Flare VM dan VirusTotal, ia harus mempunyai antara muka yang mudah difahami dan sederhana. Flare VM harus dihadkan kepada ciri-ciri yang penting dan mudah digunakan untuk mengelakkan kebingungan dalam proses analisis. VirusTotal juga harus menyediakan maklumat hasil pengesanan dengan cara yang jelas dan mudah diinterpretasikan. Rangka kerja NIST berikutnya, Mengesan (Detect) menekankan pengecaman dan pengesanan secara awal terhadap ancaman siber. Melalui penggunaan teknologi yang sesuai dan mesra pengguna, PKS dapat dengan mudah mengesan dan mengatasi ancaman siber sebelum kesan serius berlaku.

Pada keseluruhannya, model "People, Process, Technology" memerlukan pendekatan yang selaras dengan keperluan pengguna akhir dalam PKS. Proses-proses yang disyorkan harus mudah diikuti oleh pengguna akhir, dan penggunaan teknologi harus sesuai dengan kemampuan mereka tanpa menimbulkan beban tambahan kepada

PKS. Melalui kombinasi rangka kerja NIST dan model "People, Process, Technology," PKS dapat meningkatkan keselamatan siber mereka dan membina persekitaran digital yang selamat dan beretika tanpa mengorbankan kelancaran operasi perniagaan.

4.3 HUBUNGAN PENGGUNA AKHIR BERDASARKAN RANGKA KERJA KESELAMATAN SIBER NIST

Rajah 4.2 Keselamatan Siber NIST Versi Rangka Kerja 1.1

Rangka Kerja Keselamatan Siber NIST 1.1 (Rajah 4.2) adalah versi terkini yang dikeluarkan oleh National Institute of Standards and Technology (NIST) di Amerika Syarikat pada April 2018. Ia merangkumi beberapa penambahbaikan dan penambahbaikan berdasarkan maklum balas dan pengajaran yang diperoleh daripada pelaksanaan rangka kerja asal. (NIST, 2019)

Teras Rangka Kerja Keselamatan Siber NIST 1.1 terdiri daripada lima fungsi: Kenal pasti, Lindungi, Mengesan, Bertindak Balas dan Pulih, yang mewakili aktiviti utama yang terlibat dalam menguruskan risiko keselamatan siber. (NIST, 2019)

Rajah 4.3 Hubungan antara Rangka Kerja Keselamatan Siber NIST dan elemen "Pengguna Akhir"

Dalam Rajah 4.3, elemen “Pengguna Akhir” telah diutamakan dalam hubungan antara lima fungsi: Kenal Pasti, Lindungi, Mengesan, Bertindak Balas dan Pulihkan. Fungsi-fungsi ini saling berkaitan, mewakili sifat kitaran aktiviti keselamatan siber.

Dalam Rangka Kerja Keselamatan Siber NIST, pengguna akhir memainkan peranan penting dalam postur keselamatan siber keseluruhan sesebuah PKS. Walaupun rangka kerja ini memberi tumpuan terutamanya kepada menyediakan panduan kepada PKS untuk menguruskan risiko keselamatan siber, ia secara tidak langsung menangani peranan pengguna akhir dalam beberapa cara. Berikut adalah beberapa aspek rangka kerja keselamatan siber NIST yang berkaitan dengan pengguna akhir:

Fungsi "Kenal Pasti" dalam rangka kerja keselamatan siber NIST melibatkan pemahaman dan pengurusan risiko keselamatan siber. Salah satu aspek pengenalpastian risiko adalah menyedari bahawa pengguna akhir boleh menjadi kelemahan yang berpotensi. PKS harus mengenal pasti pelbagai jenis pengguna akhir, peranan mereka, dan potensi risiko yang berkaitan dengan tindakan atau tingkah laku mereka.

Fungsi "Lindungi" menekankan pelaksanaan perlindungan untuk melindungi daripada ancaman siber. Ini termasuk melaksanakan program kesedaran keselamatan dan latihan untuk pengguna akhir. PKS harus menyediakan pengguna akhir dengan pengetahuan dan kemahiran yang diperlukan untuk mengenal pasti dan mengurangkan risiko keselamatan siber. Latihan boleh merangkumi topik seperti kebersihan kata laluan, kesedaran pancingan data, amalan penyemakan imbas selamat dan pengendalian maklumat sensitif yang betul.

Fungsi "Mengesan" memberi tumpuan kepada mengenal pasti peristiwa keselamatan siber. Pengguna akhir boleh menyumbang kepada pengesanan kejadian yang berpotensi dengan menyedari dan melaporkan aktiviti yang mencurigakan, seperti e-mel pancingan data, percubaan akses yang tidak dibenarkan, atau tingkah laku sistem yang luar biasa. PKS harus menggalakkan pengguna akhir untuk segera melaporkan sebarang aktiviti mencurigakan atau anomali yang mereka hadapi.

Fungsi "Bertindak Balas" menangani tindakan yang diambil selepas pengesanan insiden keselamatan siber. Ini termasuk prosedur tindak balas insiden yang melibatkan pengguna akhir. PKS harus menentukan peranan dan tanggungjawab pengguna akhir semasa tindak balas insiden dan memberikan panduan yang jelas mengenai insiden pelaporan dan mengikuti protokol yang ditetapkan. Pengguna Akhir boleh membuat laporan kepada pihak berkuasa yang berkaitan di Malaysia seperti disediakan di Lampiran I.

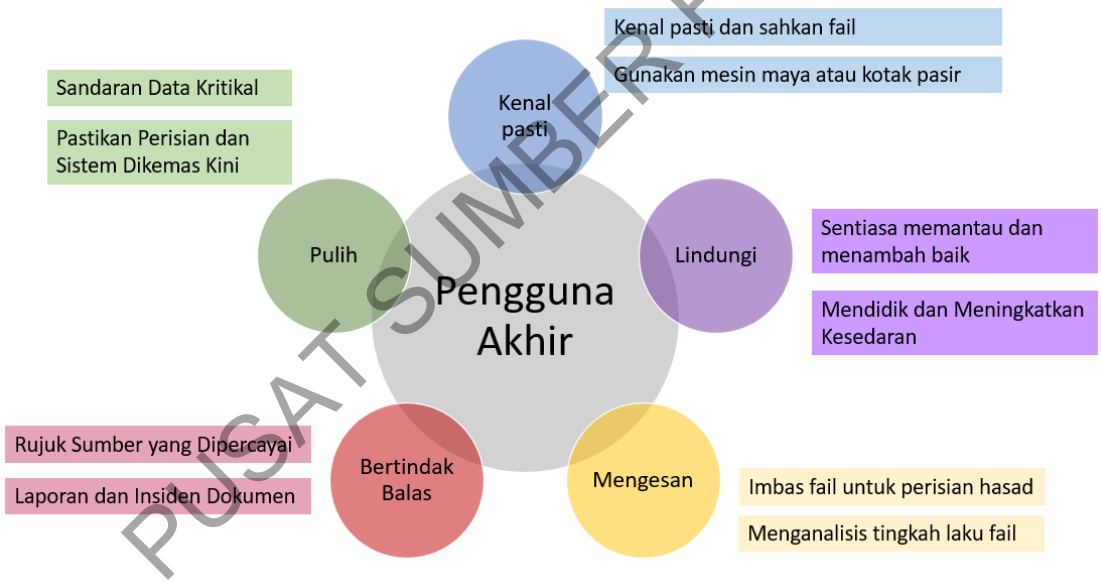
Di samping itu, di seluruh rangka kerja keselamatan siber NIST, terdapat pengiktirafan bahawa keselamatan siber adalah tanggungjawab bersama di seluruh PKS, termasuk pengguna akhir. Walaupun tanggungjawab utama untuk melaksanakan kawalan keselamatan siber terletak pada pengurusan PKS dan pasukan IT, pengguna akhir adalah sebahagian daripada ekosistem dan harus terlibat, berpendidikan, dan digalakkan untuk mengamalkan tingkah laku yang selamat.

Dengan mempertimbangkan peranan pengguna akhir dalam rangka kerja dan melaksanakan langkah-langkah latihan, kesedaran, dan tindak balas insiden yang

sesuai, PKS dapat meningkatkan daya tahan keselamatan siber mereka secara keseluruhan.

4.4 LANGKAH-LANGKAH DICADANGKAN UNTUK PENGGUNA AKHIR

Rajah 4.4 berikut adalah langkah-langkah yang menyesuaikan rangka kerja keselamatan siber NIST yang direka untuk pengguna akhir yang bekerja di PKS yang mempunyai pengetahuan teknikal dan set kemahiran yang terhad dalam keselamatan siber. Langkah-langkah ini direka dengan cara yang mudah diikuti dan ia tidak memerlukan peralatan teknologi tinggi, perkakasan atau perisian yang mahal. Ini tidak akan membebankan PKS.



Rajah 4.4 Langkah-langkah dicadangkan kepada Pengguna Akhir berdasarkan Rangka Kerja Keselamatan Siber NIST

1. Kenal pasti dan sahkan fail

Apabila menemui fail yang tidak diketahui, mulakan dengan mengesahkan sumber dan kesahihannya. Hanya muat turun atau buka fail daripada sumber yang dipercayai. Semak metadata fail, seperti nama fail, sambungan fail dan tandatangan digital (jika tersedia), untuk memastikan ia sejajar dengan jenis fail yang dijangkakan.

2. Imbas fail untuk perisian hasad

Lakukan imbasan perisian hasad pada fail menggunakan perisian antivirus atau anti-perisian hasad yang terkini. Pastikan perisian antivirus dikonfigurasikan untuk mengemas kini definisi virus secara automatik untuk mengesan ancaman terkini.

3. Gunakan mesin maya atau kotak pasir

Jika tersedia, pertimbangkan untuk menggunakan persekitaran kotak pasir atau mesin maya untuk membuka dan menganalisis fail dalam suasana terpencil dan terkawal. Ini membantu mengandungi sebarang aktiviti berniat jahat yang berpotensi dan melindungi sistem pengguna daripada bahaya.

4. Menganalisis tingkah laku fail

Jika fail itu mencurigakan atau menimbulkan kebimbangan, analisis tingkah lakunya menggunakan alat atau perkhidmatan pengesanan berasaskan tingkah laku. Alat ini memantau tindakan dan interaksi fail dengan sistem untuk mengesan sebarang tingkah laku berniat jahat atau tidak dijangka.

5. Rujuk Sumber yang Dipercayai

Jika pengguna tidak pasti tentang fail atau memerlukan bantuan lanjut, rujuk sumber yang dipercayai seperti Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM), forum keselamatan siber, atau profesional IT dalam organisasi. Dapatkan nasihat dan panduan pakar untuk memastikan pengendalian fail yang selamat.

6. Laporan dan Insiden Dokumen

Jika pengguna menemui fail yang disahkan atau disyaki berniat jahat, laporkan kejadian itu kepada pasukan IT, keselamatan organisasi, atau Polis Diraja Malaysia (PDRM) mengikut prosedur tindak balas insiden yang telah ditetapkan. Berikan maklumat terperinci tentang fail, sumbernya, dan sebarang tingkah laku yang diperhatikan.

Mendokumenkan kejadian itu untuk rujukan dan analisis masa depan. Terdapat lebih banyak cara untuk melaporkan insiden disenaraikan dalam Lampiran I.

7. Mendidik dan Meningkatkan Kesedaran

Sentiasa mendidik pengguna akhir tentang amalan terbaik pengendalian fail, termasuk risiko yang berkaitan dengan fail yang tidak diketahui atau berniat jahat. Menjalankan sesi latihan, mengedarkan bahan pendidikan, dan mempromosikan budaya kesedaran keselamatan siber dalam organisasi.

8. Pastikan Perisian dan Sistem Dikemas Kini

Pastikan sistem pengendalian, aplikasi dan perisian keselamatan anda dikemas kini dengan tampalan dan kemas kini terkini. Sentiasa pasang kemas kini keselamatan dan dayakan kemas kini automatik jika boleh untuk melindungi daripada kelemahan yang diketahui.

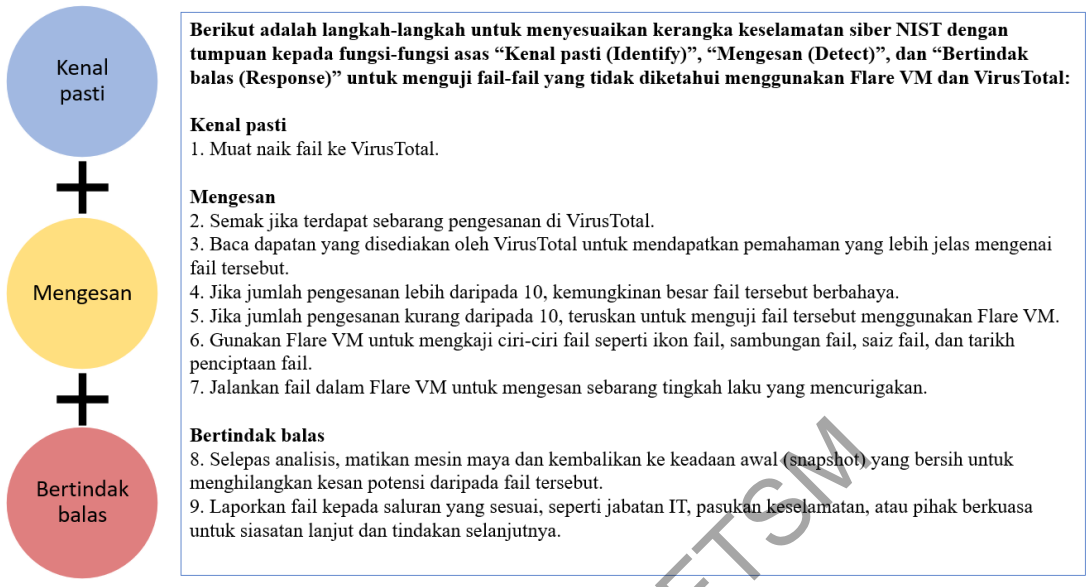
9. Sandaran (Backup) Data Kritikal

Sentiasa sandarkan (backup) data kritikal anda ke lokasi yang berasingan dan selamat. Sekiranya berlaku jangkitan perisian hasad atau kehilangan data, mempunyai sandaran (backup) baru-baru ini memastikan bahawa anda boleh memulihkan fail penting anda tanpa bergantung pada versi yang berpotensi terjejas.

10. Sentiasa memantau dan menambah baik

Sentiasa memantau dan menilai keberkesanan metodologi. Dapatkan maklum balas daripada pengguna akhir dan pasukan IT/keselamatan untuk mengenal pasti kawasan untuk penambahbaikan. Kekal dikemas kini dengan garis panduan NIST terkini dan sesuaikan metodologi dengan sewajarnya untuk menangani ancaman dan cabaran yang muncul dicadangkan

4.5 LANGKAH-LANGKAH YANG FOKUS DALAM EKSPERIMEN



Rajah 4.5 Langkah-Langkah yang fokus dalam eksperimen

Berikut adalah prosedur yang direka dan dicadangkan untuk pengguna akhir untuk mengesan fail-fail yang tidak diketahui. Seperti yang ditunjukkan dalam Rajah 4.5 langkah-langkah yang memberi tumpuan dalam eksperimen telah dihuraikan seperti berikut:

1. [**Kenal pasti**] Muat naik fail ke VirusTotal: Langkah pertama dalam prosedur ini adalah muat naik fail yang mencurigakan ke laman web VirusTotal. Untuk melakukan ini, pengguna perlu mengakses laman web VirusTotal dan pilih opsyen muat naik untuk fail yang ingin dianalisis.

2. [**Mengesan**] Semak jika terdapat sebarang pengesanan di VirusTotal: Selepas fail dimuat naik ke VirusTotal, alat ini akan melakukan pengesanan terhadap fail tersebut dengan menggunakan pelbagai enjin antivirus dan mekanisme pengesanan lainnya. Pengguna perlu menyemak hasil pengesanan untuk melihat sama ada terdapat sebarang tanda-tanda kehadiran perisian hasad atau ancaman siber dalam fail tersebut.

3. [**Mengesan**] Baca dapatan yang disediakan oleh VirusTotal untuk mendapatkan pemahaman yang lebih jelas mengenai fail tersebut: VirusTotal akan menyediakan dapatan dan maklumat yang diperoleh daripada hasil pengesanan.

Pengguna perlu membaca dan memahami maklumat ini untuk mendapatkan gambaran yang lebih jelas mengenai sifat dan potensi risiko fail yang dikaji.

4. [**Mengesan**] Jika jumlah pengesanan lebih daripada 10, kemungkinan besar fail tersebut berbahaya: Jika terdapat banyak pengesanan yang mengenal pasti fail sebagai berbahaya atau berpotensi berbahaya, pengguna perlu mengambil langkah berjaga-jaga dan menganggap bahawa fail tersebut mungkin mengandungi perisian hasad atau ancaman serius.

5. [**Mengesan**] Jika jumlah pengesanan kurang daripada 10, teruskan untuk menguji fail tersebut menggunakan Flare VM: Jika terdapat sedikit atau tiada pengesanan yang mencurigakan dalam VirusTotal, langkah seterusnya adalah meneruskan analisis fail tersebut menggunakan Flare VM. Langkah ini diambil kerana ada kemungkinan bahawa perisian hasad tersebut mungkin belum diketahui oleh enjin pengesan dalam pangkalan data VirusTotal.

6. [**Mengesan**] Gunakan Flare VM untuk mengkaji ciri-ciri fail seperti ikon fail, sambungan fail, saiz fail, dan tarikh penciptaan fail: Flare VM adalah mesin maya yang membolehkan pengguna untuk meneroka lebih mendalam ciri-ciri fail yang mencurigakan. Dalam langkah ini, pengguna perlu mengkaji ikon fail, sambungan fail, saiz fail, dan tarikh penciptaan fail untuk mencari petunjuk tambahan tentang potensi ancaman yang ada.

7. [**Mengesan**] Jalankan fail dalam Flare VM untuk mengesan sebarang tingkah laku yang mencurigakan: Setelah memeriksa ciri-ciri fail, langkah seterusnya adalah menjalankan fail tersebut dalam persekitaran terkawal Flare VM. Tujuannya adalah untuk mengesan sebarang tingkah laku atau tindakan mencurigakan yang mungkin dilakukan oleh fail tersebut.

8. [**Bertindak balas**] Selepas analisis, matikan mesin maya dan kembalikan ke keadaan awal (snapshot) yang bersih untuk menghilangkan kesan potensi daripada fail tersebut: Setelah analisis selesai, pengguna perlu mematikan Flare VM dan mengembalikannya kepada keadaan awal (snapshot) yang bersih sebelum analisis. Ini bertujuan untuk menghilangkan sebarang kesan yang mungkin ditinggalkan oleh fail mencurigakan tersebut dalam sistem.

9. [**Bertindak balas**] Laporkan fail kepada saluran yang sesuai, seperti jabatan IT, pasukan keselamatan, atau pihak berkuasa untuk siasatan lanjut dan tindakan selanjutnya: Jika pengguna mendapati bahawa fail tersebut memang mengandungi perisian hasad atau ancaman siber, mereka perlu melaporkannya kepada saluran yang sesuai seperti jabatan IT, pasukan keselamatan, atau pihak berkuasa untuk tindakan lanjut dan langkah-langkah pemulihan atau penambahbaikan yang diperlukan.

4.6 KESIMPULAN

Secara kesimpulannya, langkah-langkah di dalam elemen “Kenal pasti”, “Mengesan” dan “Bertindak Balas” akan dititikberatkan. Projek ini bertujuan untuk membantu pengguna akhir terutamanya yang berkhidmat di PKS mengenal pasti dan mengesan fail yang tidak diketahui, oleh itu, prosedur yang telah dinyatakan di atas dicadangkan. Prosedur yang dicadangkan akan menggabungkan rangka kerja keselamatan siber NIST yang diiktiraf oleh industri. Prosedur yang dicadangkan ini disesuaikan sebagai yang mudah, terang, dan jelas dengan mempertimbangkan tahap kepakaran pengguna akhir serta halangan yang dihadapi oleh PKS. Prosedur yang dicadangkan akan diuji dalam bab seterusnya.

BAB V

EKSPERIMEN, KEPUTUSAN DAN PERBINCANGAN

5.1 PENGENALAN

Bab ini akan membentangkan dan menganalisis keputusan eksperimen. Bab ini terdiri daripada dua bahagian: bahagian hasil, di mana data yang telah dikumpulkan dan dianalisis dibentangkan, dan bahagian perbincangan, di mana penemuan ditafsirkan dan langkah-langkah untuk pengguna akhir dibincangkan.

5.2 KEPUTUSAN KAJIAN

Hasil eksperimen ini akan memberi tumpuan kepada tanda-tanda yang dikumpulkan dari VirusTotal. Ini kerana mesin maya Flare VM bertujuan melihat pelaksanaan perisian hasad, bagaimana rupanya dan bagaimana ia akan dilaksanakan dalam persekitaran terpencil dan terkawal. Oleh kerana Flare VM bukan kotak pasir perisian hasad, ia tidak disertakan dengan ciri pelaporan. Oleh itu, dalam bab ini, hasil eksperimen akan berdasarkan terutamanya dari VirusTotal

Terdapat sejumlah 576 perisian hasad yang dimuat naik ke VirusTotal. Jadual 5.1 berikut ialah kiraan pengesanan perisian hasad pada jumlah fail perisian hasad. Pengesanan perisian hasad tertakluk pada masa fail diserahkan kepada laman sesawang VirusTotal. Kadang-kadang, butang "dianalisis semula" (Reanalyzed) digunakan untuk mendapatkan pengesanan perisian hasad terkini daripada VirusTotal.

Jadual 5.1 Kiraan pengesanan perisian hasad di VirusTotal

Kiraan Pengesanan di VirusTotal	Jumlah Perisian Hasad
0 - 10	34
11 - 20	3
21 - 30	5
31 - 40	22
41 - 50	34
51 - 60	240
61 - 70	238

Di VirusTotal, terdapat kira-kira 70 pengimbas perisian hasad yang tersedia untuk mengimbas fail yang dimuat naik. Terdapat 238 fail yang dikenal pasti sebagai perisian hasad dengan mempunyai 61-70 tandatangan pengesanan perisian hasad. Kemudian, terdapat 240 fail yang dikenal pasti dengan mempunyai 51-60 tandatangan pengesanan perisian hasad. Di sisi lain, terdapat 34 fail yang hanya dikesan oleh 0-10 pengimbas perisian hasad di VirusTotal. Ini menunjukkan fail-fail tersebut kurang berbahaya.

Majoriti fail perisian hasad didapati mengandungi lebih daripada satu kategori ancaman. Berdasarkan pengiraan, setiap perisian hasad menemui 1 - 3 kategori ancaman. Rajah 5.1 berikut adalah carta ringkasan.

Akan tetapi, terdapat 19 fail yang tidak mempunyai kategori ancaman dalam VirusTotal, ini tidak bermakna fail tersebut tidak berbahaya; mereka cuma mempunyai pengesanan yang kurang untuk diklasifikasikan dengan mana-mana kategori ancaman.