ANALISIS TINGKAH LAKU PERISIAN HASAD MENGGUNAKAN VISUALISASI

LUQMAN HARIZ BIN MAT BARHAN
WAN FARIZA PAIZI @ FAUZI

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Salah satu risiko kepada keselamatan maklumat yang terus berkembang ialah perisian hasad. Lebih banyak sistem dan peranti telah dijangkiti perisian hasad sejak Wannacry.exe yang terkenal dan permulaan wabak covid-19. Berdasarkan artikel "Statistik dan fakta perisian hasad untuk 2022" daripada comparitech tapak web, pada tahun 2020, 61% organisasi melaporkan aktiviti perisian hasad yang merebak dari seorang pekerja ke pekerja seterusnya. Pada tahun 2021, angka itu meningkat kepada 74%, dan pada tahun 2022, ia mencapai 75%, kadar jangkitan tertinggi sejak tinjauan Perusahaan Milik Negara (SOE) bermula pada 2016. Oleh kerana perisian hasad komputer merebak dengan cepat ke seluruh rangkaian, peranti sistem keselamatan seperti anti-virus, tembok api dan sistem pengesanan pencerobohan (IDS) dianggap tidak dapat mengesan perisian hasad yang lebih baharu disebabkan teknik pengelakan yang lebih baik yang diumumkan oleh Picus Security daripada laman web Help Nets Security. Ini mengakibatkan kehilangan data yang ketara dan kerugian kewangan bagi banyak organisasi. Matlamat projek ini adalah untuk membina sebuah perisian yang mengvisualisasi tingkah laku pelbagai jenis perisian hasad. Kami juga akan menyiasat tingkah laku rangkaian mereka kerana akses rangkaian adalah salah satu gelagat penting perisian hasad. Analisis yang terhasil boleh digunakan untuk membangunkan skim pengesanan perisian hasad atau untuk tujuan pembelajaran, terutamanya untuk pentadbir rangkaian, penganalisis keselamatan siber dan pelajar. Sampel perisian hasad terbaharu akan dikumpulkan daripada Laman Web Arkib Perisian Hasad dan GitHub. Kemudian, dua jenis analisis malware akan dilakukan iaitu analisis statik dan analisis dinamik. Analisis statik meneliti kod fail perisian hasad tanpa melaksanakannya menggunakan pelbagai teknik seperti pembongkar. Manakala analisis dinamik dilakukan dengan menjalankan perisian hasad dalam sistem selamat seperti mesin maya dan memantau proses perisian hasad dan paket data yang dihasilkan olehnya. Pada akhir penyelidikan, hasilnya divisualisasikan dari segi garis masa jangkitan perisian hasad yang termasuk tingkah laku, pencetus dan penunjuk kompromi (IOC) untuk memberikan lebih banyak cerapan tentang perisian hasad.

PENGENALAN

Perisian hasad merujuk kepada perisian berniat jahat yang direka untuk merosakkan atau mengeksploitasi peranti, perkhidmatan, atau rangkaian komputer. Penjenayah siber menggunakan perisian hasad untuk mencuri maklumat peribadi, seperti data kewangan, e-mel, dan kata laluan mangsa. Terdapat pelbagai jenis perisian hasad, termasuk virus, trojan, perisian tebusan, botnet, dan lain-lain. Setiap tahun, jumlah bilangan perisian hasad baharu yang dihasilkan dan tersebar ke rangkaian organisasi bertambah. Perisian hasad sedia ada berkembang dalam strukturnya, menjadikan pengesanannya lebih sukar berbanding sebelum ini. Menurut SonicWall, 270,228 varian perisian hasad "tidak pernah dilihat sebelum ini" ditemui pada separuh pertama tahun 2022 sahaja. Ia merupakan peningkatan 45% berbanding tempoh yang sama tahun lepas (2021), dengan lebih 1,500 varian baharu ditambah setiap hari. Pada Mac 2022 sahaja, hampir 60,000 varian baharu ditemui, mencatat rekod tinggi baharu. Pengesanan perisian hasad menggunakan teknik pengesanan asas dan lanjutan, termasuk kecerdasan buatan dan pembelajaran mesin. Analisis perisian hasad memeriksa tingkah laku dan sifat statik perisian tersebut untuk mengenali ancaman dan menentukan langkah keselamatan. Jumlah varian perisian hasad baharu terus meningkat setiap tahun, dan pengesanan serta perlindungannya menjadi semakin mencabar. Oleh itu, menyediakan maklumat analisis perisian hasad yang komprehensif penting untuk memahami potensi kerosakan atau kecurian data yang mungkin disebabkan oleh perisian hasad.

PENYATAAN MASALAH

Analisis perisian hasad melibatkan penggunaan alat-alat penganalisis seperti Cuckoo Sandbox, VirusTotal, PeStudio, Ghidra, dan x64dbg. Cuckoo adalah sistem analisis perisian hasad automatik sumber terbuka yang dapat menganalisis fail secara otomatis dan mengumpulkan hasil analisis yang komprehensif tentang tingkah laku perisian hasad. VirusTotal memindai fail/url dari sumber yang tidak diketahui menggunakan 70 pengimbas antivirus dan melaporkan apakah fail itu bersih atau berniat jahat. PeStudio membantu penganalisis mencari artefak mencurigakan dalam fail boleh laku untuk mempercepat penilaian perisian hasad. Ghidra dan x64dbg adalah alat kejuruteraan terbalik yang membolehkan penganalisis menyahpepijat dan menganalisis perisian. Ghidra menawarkan berbilang platform dan seni bina, termasuk x86, ARM, dan MIPS, sementara x64dbg membolehkan penganalisis melangkah melalui kod, memeriksa memori, dan mendaftar dalam masa nyata. Penganalisis perisian hasad sering menghadapi cabaran dalam menganalisis perisian yang lebih baharu, yang sering menggunakan teknik "packing" atau kekeliruan untuk menyulitkan analisis. Hasil analisis perisian hasad dijana dalam bentuk laporan teks yang dapat memerlukan penelitian lebih lanjut. Penjenayah siber juga terus mencari cara baru untuk mengelakkan pengesan perisian hasad dengan memperbaharui dan menyusun semula kaedah mereka. Oleh itu, penganalisis harus selalu beradaptasi dan meningkatkan teknik analisis mereka untuk menghadapi ancaman yang semakin canggih.

OBJEKTIF KAJIAN

Antara objektif kajian ini :

- Untuk menyiasat pelbagai teknik dan alatan analisis perisian hasad.
- Untuk menganalisis perisian hasad untuk menentukan cara sistem telah dijangkiti oleh perisian hasad.
- Untuk visualisasi aktiviti jangkitan perisian hasad berdasarkan tingkah lakunya.

SOROTAN SASTERA

Kajian susastera ialah bab yang memfokuskan kepada penyelidikan projek peningkatan kualiti dengan merujuk kepada beberapa sumber maklumat sahih seperti artikel, jurnal, tesis penyelidikan dan aplikasi atau alatan yang berkait rapat dengan penyelidikan projek analisis perisian hasad ini. Dalam bab ini, maklumat lanjut tentang jenis perisian hasad, jenis kaedah analisis perisian hasad dan jenis graf data visualisasi akan dibincangkan untuk mendapatkan dan memahami sepenuhnya struktur perisian hasad.

Juga dalam bab ini, kami akan membandingkan teknik visualisasi yang tersedia untuk analisis perisian hasad dan memilih teknik terbaik yang akan digunakan berdasarkan penemuan kami daripada sumber yang berbeza.

LATAR BELAKANG

Pencipta perisian hasad secara aktif cuba mereka bentuk perisian hasad menggunakan cara “packing” atau kekeliruan (obfuscation) untuk menjadikan fail mereka lebih sukar untuk dikesan atau dianalisis. Ini menyebabkan proses untuk penganalisis mengesan perisian hasad

yang lebih baharu menjadi perlahan kerana ia mengambil masa untuk menganalisis kaedah khusus yang akan digunakan oleh perisian hasad yang mana ia mewujudkan selang masa antara pelepasan sampel baharu dan pelepasan tandatangan baharu. Oleh itu, amalan terbaik dalam mengesan perisian hasad baharu adalah untuk memahami cara setiap jenis perisian hasad berfungsi dan dengan memperoleh pengetahuan ini, penganalisis boleh memahami lebih lanjut dengan memperoleh setiap butirannya yang boleh ditukar menjadi data visualisasi untuk gambaran keseluruhan yang lebih baik.

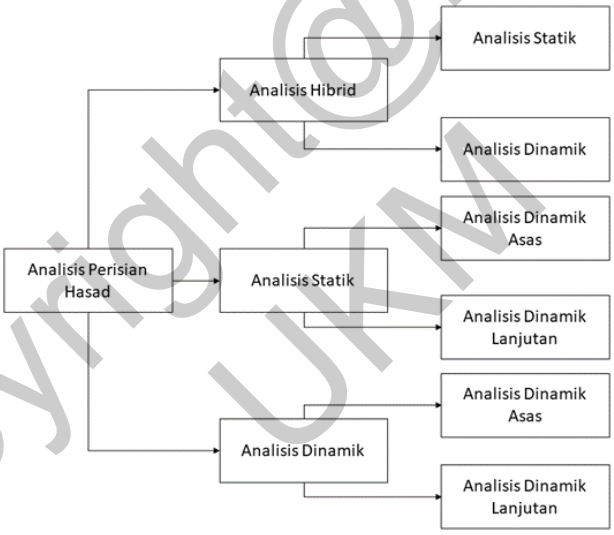
JENIS-JENIS PERISIAN HASAD

Setiap perisian hasad mempunyai cara dan matlamat tersendiri untuk menyerang sistem. Perisian hasad boleh dikelaskan kepada beberapa jenis iaitu Virus, Perisian tebusan (Ransomware), Kuda Trojan, Cecacing Komputer, Bot, Perisian pengintip dan Perisian Iklan. Setiap serangan perisian hasad mempunyai set objektif dan sasarannya sendiri, dan semuanya amat berbahaya kepada perniagaan. Walau bagaimanapun, dalam kes ini, kami telah memutuskan untuk melaksanakan visualisasi analisis perisian hasad untuk projek ini menggunakan satu jenis perisian hasad iaitu kuda trojan. Trojan biasanya digunakan dalam analisis perisian hasad kerana ia berfungsi sebagai alat penting untuk memahami dan mengkaji tingkah laku perisian hasad. Apabila mengkaji perisian hasad, penyelidik keselamatan dan penganalisis perlu memerhatikan tindakannya dalam persekitaran terkawal tanpa berisiko merosakkan sistem sebenar. Trojan menyediakan cara untuk melaksanakan perisian hasad dalam persekitaran kotak pasir atau terpencil, membenarkan penganalisis memantau aktivitinya, merekodkan tingkah lakunya dan mengumpulkan maklumat penting seperti protokol komunikasi, pelayan arahan dan kawalan dan potensi muatan. Pendekatan ini membantu penyelidik mendapatkan cerapan tentang fungsi perisian hasad, teknik jangkitan dan

taktik pengelakan, membolehkan mereka membangunkan langkah balas yang berkesan dan meningkatkan keselamatan siber secara keseluruhan.

KAEDAH ANALISIS PERISIAN HASAD

Apabila kita ingin melakukan analisis perisian hasad, kita mesti terlebih dahulu memahami teknik yang digunakan yang telah kami pilih untuk digunakan dalam projek ini. Terdapat tiga teknik utama untuk menganalisis perisian hasad, kaedah yang paling banyak digunakan ialah analisis statik, analisis dinamik dan analisis hibrid. Kaedah analisis perisian hasad ditunjukkan di bawah dalam rajah 2.1.

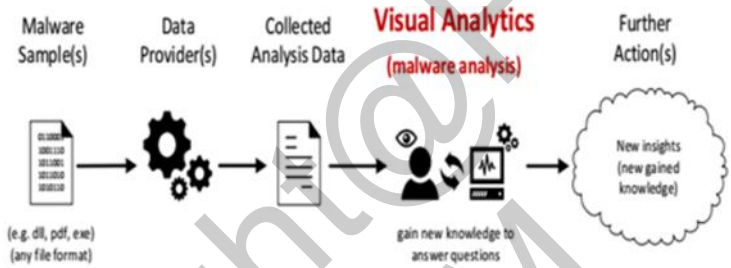


Rajah 1 Kaedah Analisis Perisian Hasad

TEKNIK PENGESANAN PERISIAN HASAD

Menurut sastera sedia ada, enam kategori utama teknik pengesanan digunakan untuk mengesan, mengelas dan mengenal pasti perisian hasad. Pengkategorian teknik yang digunakan untuk pengesanan perisian hasad adalah berdasarkan kaedah pengesanan. Iaitu

Berasaskan Tandatangan, Berasaskan Tingkah Laku, Berasaskan Analisis, Berasaskan Pembelajaran Mesin, Berasaskan Anomali dan Berasaskan Visualisasi. Menurut kajian kes terdahulu, teknik visualisasi boleh digunakan untuk mentakrifkan tindakan yang disyaki dan tindak balas terhadapnya secara serentak dalam situasi keselamatan. Menggunakan teknik sedemikian bertujuan untuk membantu penganalisis mempertimbangkan dan mengklasifikasikan jenis perisian hasad dengan cepat. Visualisasi membantu penganalisis memahami perisian hasad secara grafik dengan menyerlahkan IOC utama dan aliran proses tingkah laku yang tidak boleh dilakukan dalam bentuk analisis perisian hasad yang lain.



Rajah 2 Aliran Kerja Umum Pengesanan Perisian Hasad Menggunakan Teknik Visualisasi

TEKNIK VISUALISASI DATA

Penganalisis boleh mendapat manfaat daripada kaedah visualisasi, yang merupakan teknik berguna untuk mencirikan tindakan yang disyaki dan tindak balas terhadapnya pada masa yang sama. Menggunakan teknik sedemikian bertujuan untuk membantu penganalisis mempertimbangkan dan mengklasifikasikan jenis perisian hasad dengan laju. Terdapat pelbagai kaedah untuk visualisasi data, seperti bar, pai, kawasan, piza, grafik garis dan titik, dan penghirisan isipadu (volume) dalam 3D untuk mewakili imej dwi-dimensi, yang boleh digunakan untuk menggambarkan tindakan perisian hasad. Pada masa ini, terdapat beberapa teknik visualisasi perisian hasad yang didokumenkan dalam penyelidikan perisian hasad.

Antaranya ialah Peta Pokok Perisian Hasad, Graf Benang Perisian Hasad, Imej Perisian Hasad, Graf Terpaut, Gambar Rajah Sankey Perisian Hasad dan Graf Pengetahuan.

PERBANDINGAN DAN PERBEZAAN

Dalam bahagian ini, kami akan membandingkan teknik visualisasi perisian hasad sedia ada dan jenis analisis perisian hasad yang telah disebut di latar belakang. Teknik visualisasi perisian hasad berdasarkan ciri perisian hasad dinamik termasuk Peta Pokok Perisian Hasad, Graf Benang Perisian Hasad, Graf Terpaut dan Gambar Rajah Sankey. Ia memaparkan data yang berubah dari semasa ke semasa tanpa memerlukan interaksi pengguna. Imej Hasad, sebaliknya, ialah teknik visualisasi perisian hasad berdasarkan ciri statik. Data dipetakan untuk memaparkan ruang dan pembolehubah visual tidak berubah yang lain. Interaktiviti tidak dikecualikan oleh pemetaan statik; ia masih boleh diubah suai melalui interaksi pengguna. Jadual 1 menunjukkan perbandingan antara teknik visualisasi perisian hasad sedia ada dan atributnya berdasarkan penyelidikan yang telah ditemui.

Jadual 1 Perbandingan Teknik Visualisasi Perisian Hasad Sedia Ada

Teknik Visualisasi	Jenis Ciri-ciri yang Digunakan	Ciri-ciri yang Digunakan	Had
Peta Pokok Perisian Hasad	Dinamik	Panggilan API	Butir-butiran yang rendah,Tiada urutan maklumat
Graf Benang Perisian Hasad	Dinamik	Panggilan API	Butir-butiran yang rendah, Terhad kepada 550 operasi

Imej Hasad	Statik	Perisian Hasad Mentah Binari	Tidak mewakili tingkah laku perisian hasad sebenar
Graf Berpaut	Dinamik	Alamat IP (Protokol Internet) yang diselesaikan, Nama Hos Berniat jahat	Tidak dimaksudkan untuk mewakili tingkah laku perisian hasad
Gambar Rajah Sankey (Procdot)	Dinamik	Pemantau Proses (Operasi,PID (Proses ID), Nama Proses, etc.), Aktiviti Rangkaian (Alamat IP, Nama Domain)	Menjadi berantakan (cluttered) apabila berhadapan dengan tingkah laku perisian hasad yang kompleks
Graf Pengetahuan (Knowledge Graph)	Dinamik	Pemantau Proses (Operasi,PID (Proses ID), Nama Proses, etc.), Aktiviti Rangkaian (Alamat IP, Nama Domain)	Nod menjadi tidak tersusun apabila banyak proses berlaku.

Imej Hasad tidak sesuai untuk tujuan ini kerana ia menggunakan binari perisian hasad mentah, yang tidak termasuk data tingkah laku seperti pengepala PE (metadata) dan sumber (cth ikon, peta bit, fail xml). Peta asas hasad juga tidak cukup terperinci untuk membezakan keluarga atau kumpulan hasad yang serupa kerana ia hanya mewakili tingkah laku dalam bahagian. Graf benang hasad juga mempunyai had dengan bilangan bahagian tingkah laku yang terhad. Gambar rajah Sankey boleh menunjukkan aliran proses pemprosesan hasad, tetapi ia menjadi

kucar-kacir dan sukar dibaca apabila hasad hasad mempunyai tingkah laku yang kompleks. Graf pengetahuan, walaupun ia mempunyai kuasa dalam menganalisis hubungan antara entiti, juga kurang tepat dalam menunjukkan laluan dari awal hingga akhir. Secara keseluruhannya, teknik visualisasi terbaik untuk projek ini ialah graf pengetahuan kerana keupayaannya untuk menunjukkan tingkah laku hasad tertentu dengan cara yang terperinci dan mudah difahami.

Bagi jenis analisis perisian hasad, terdapat tiga jenis analisis yang akan dibincangkan berdasarkan Jadual di bawah.

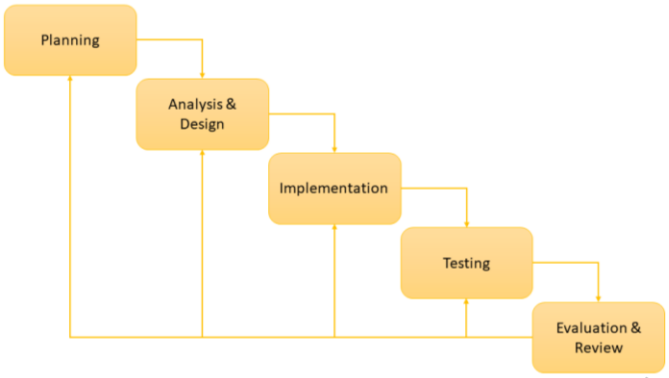
Jadual 2 Perbandingan Jenis Analisis Perisian Hasad

Faktor	Analisis Statik	Analisis Dinamik	Analisis Hibrid
Masa Diperlukan	Kurang	Lebih	Lebih
Hasil	Maklumat fail, rentetan, metadata, petunjuk kompromi (IOC)	Tingkah laku proses, lambakan memori, tangkapan rangkaian, log	Data diperoleh daripada analisis statik dan dinamik
Kekeliruan kod	Ya	Tidak	Tidak
Penggunaan Sumber (Kuasa dan Tenaga)	Kurang	Lebih	Lebih
Keberkesanan dan Ketepatan	Kurang berbanding dengan analisis dinamik	Lebih baik daripada analisis statik	Lebih baik daripada analisis statik dan dinamik

Analisis Hasad melibatkan beberapa faktor penting: masa yang diperlukan, keputusan data yang diperoleh, kekeliruan kod, penggunaan sumber seperti CPU dan RAM dan keberkesanan dan ketepatan keputusan. Dalam projek ini, analisis hibrid, yang menggabungkan analisis statik dan dinamik, adalah yang paling sesuai. Analisis statik terhad dalam penglihatan dan tidak dapat mengenal pasti masalah seperti kekeliruan kod atau fail yang tersembunyi. Analisis dinamik, walaupun ia boleh menganalisis operasi yang sedang berjalan, ia juga memerlukan kos dan masa yang tinggi serta tidak menyediakan data yang lengkap. Sebaliknya, analisis hibrid memberikan hasil yang tepat dan komprehensif, menghapuskan kelemahan analisis statik dan dinamik individu. Oleh itu, analisis hibrid adalah pilihan terbaik untuk tujuan projek ini.

METODOLOGI

Dalam projek pembangunan visualisasi analisis perisian hasad, model proses "Air Terjun Iteratif" dipilih kerana fleksibiliti yang lebih tinggi berbanding model air terjun tradisional. Model ini membolehkan penyesuaian kepada perubahan keperluan atau masalah reka bentuk yang ditemui semasa pelaksanaan. Model Air Terjun Iteratif juga mempunyai fasa perancangan, fasa keperluan dan reka bentuk, fasa pelaksanaan, dan fasa penilaian dan semakan, hampir sama dengan model air terjun tradisional. Namun, ia memberi peluang untuk maklum balas dan lelaran, mengurangkan risiko kegagalan projek.. Rajah 1.1 menunjukkan Metodologi Agile bagi projek ini.



Rajah 3 SDLC Air Terjun Berulang untuk Analisis Perisian Hasad

1 Fasa Perancangan

Fasa ini melibatkan perancangan rapi yang terdiri daripada penghasilan tajuk projek, pernyataan masalah, skop dan kekangan untuk mengetahui kebolehan melaksanakan projek ini. Dalam kes projek ini, kami telah melakukan beberapa kajian tentang isu semasa mengenai peningkatan serangan perisian hasad melalui artikel dan berita terkini mengenai peningkatan varian perisian hasad yang lebih baharu. Kami meninjau senarai 10 teratas serangan perisian hasad yang telah dilakukan pada tahun 2022.

2 Fasa Keperluan dan Reka Bentuk

Selepas perancangan rapi berkaitan maklumat yang perlu terlibat dibuat dalam fasa perancangan, fasa ini akan bermula di mana alatan, sampel dan teknik perisian hasad akan dikaji dan dikumpulkan untuk mereka bentuk rangka kerja/proses analisis perisian hasad sehingga bahagian visualisasi.

3 Fasa Perlaksanaan

Setelah fasa analisis dan reka bentuk selesai, fasa pelaksanaan akan bermula di mana pasir kotak cuckooo akan dijalankan ke atas sampel perisian hasad secara automatik. Setelah proses selesai, semua maklumat seperti pemantauan proses dan trafik rangkaian yang dikumpul akan diekstrak dalam procmon.csv bagi kesenangan untuk mengimport fail ke dalam modul visualisasi. Modul Python visualisasi tersebut akan menjana hasil visualisasi perisian hasad menggunakan Graf Pengetahuan (Knowledge Graph). Apabila proses tersebut berjaya, kesemua alatan dan modul akan disepadukan (intergrated) ke dalam kotak pasir Cuckoo.

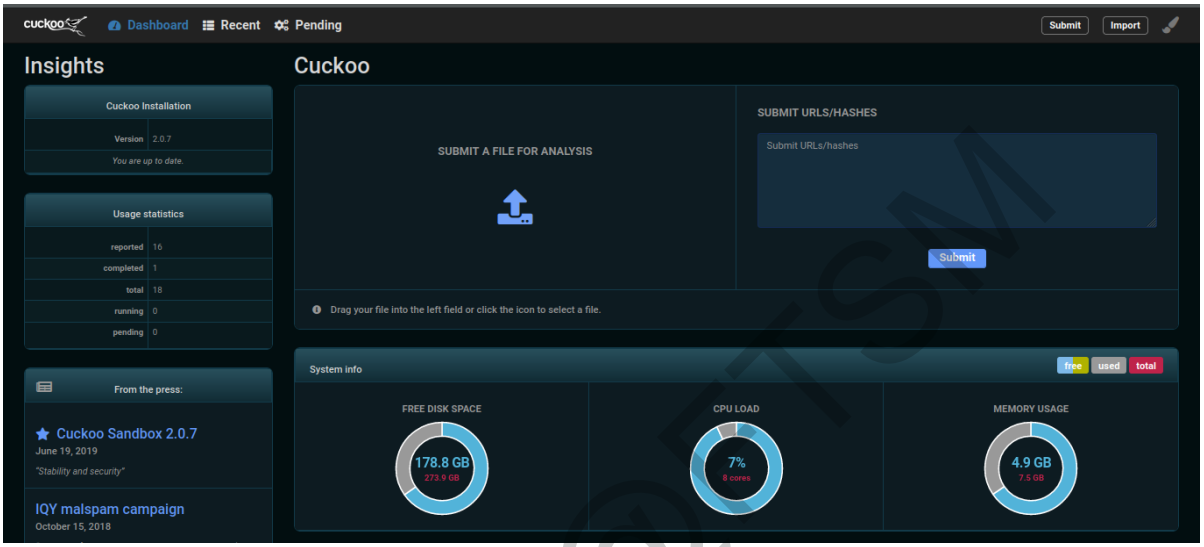
4 Fasa Penilaian dan Semakan

Semasa fasa penilaian dan semakan, laporan akan digunakan untuk menentukan sama ada keputusan analisis perisian hasad adalah setara dengan laporan yang telah kami kumpulkan berdasarkan komponen IOC, aktiviti rangkaian, pemerhatian dan tingkah laku yang digunakan oleh perisian hasad menggunakan Virus Total. Bagi graf visualisasi, keputusan tersebut akan dibezakan dengan procmon.csv untuk memastikan kesemua proses data adalah sama dengan graf.

KEPUTUSAN DAN PERBINCANGAN

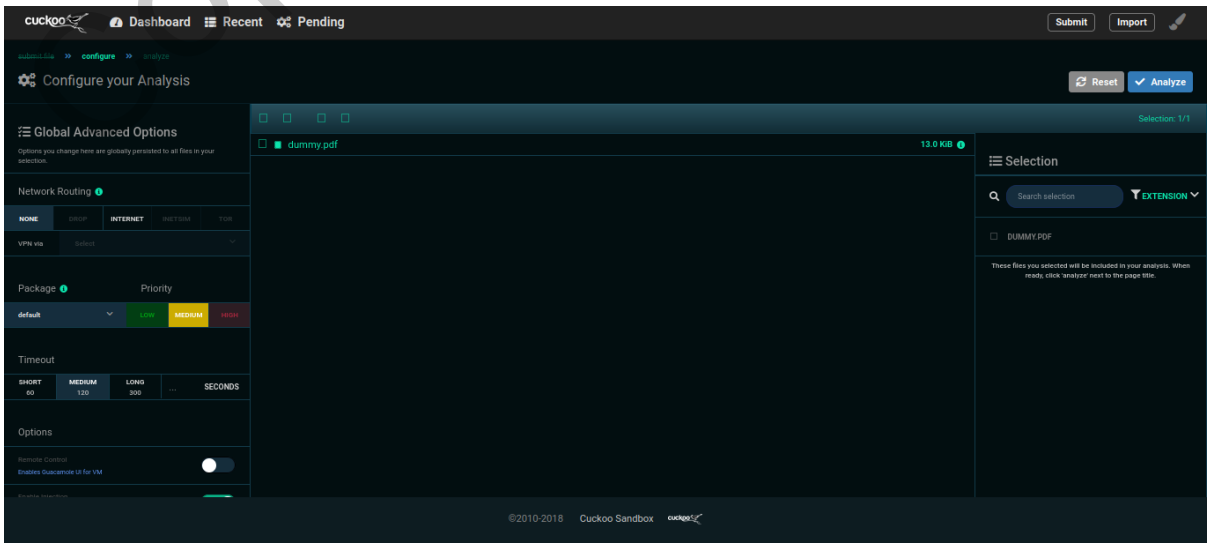
Sistem Visualisasi Analisis Perisian Hasad dibangunkan dengan menggunakan bahasa pengaturcaraan Python 2.7 dan HTML, dan penyimpanan data terletak di SQLite3 yang telah disediakan oleh kotak pasir Cuckoo dan server l*ocalhost.* Perisian yang digunakan ialah Visual Studio Code dan system operasi yang digunakan dalam pembangunan ini adalah Linux Ubuntu 18.04.

Bagi bahagian papan pemuka utama Cuckoo, terdapat beberapa komponen yang membimbing penganalisis untuk memilih tab yang hendak dituju dan dilihat. Rajah 1 menunjukkan antara muka bagi papan pemuka utama Cuckoo.



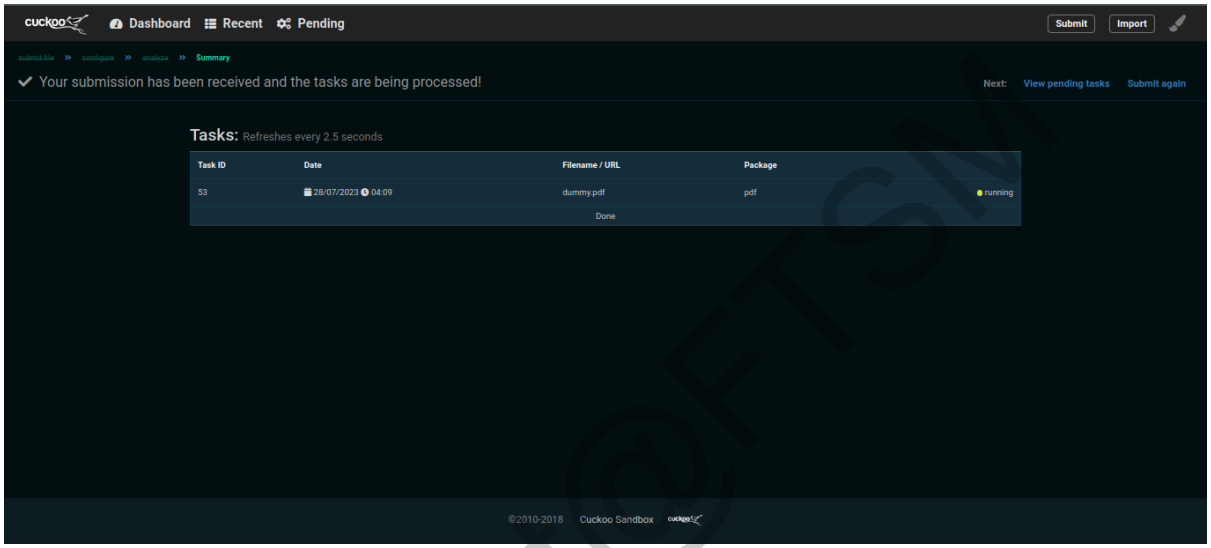
Rajah 4 Antara Muka Papan Pemuka Utama Cuckoo

Apabila penganalisis memuat naik fail ke dalam tab "*SUBMIT A FILE FOR ANALYSIS*", ia akan membawa penganalisis ke membawa penganalisis ke halaman web analisis konfigurasi seperti dalam gambar rajah di bawah.



Rajah 5 Antara Muka Konfigurasi Analisis

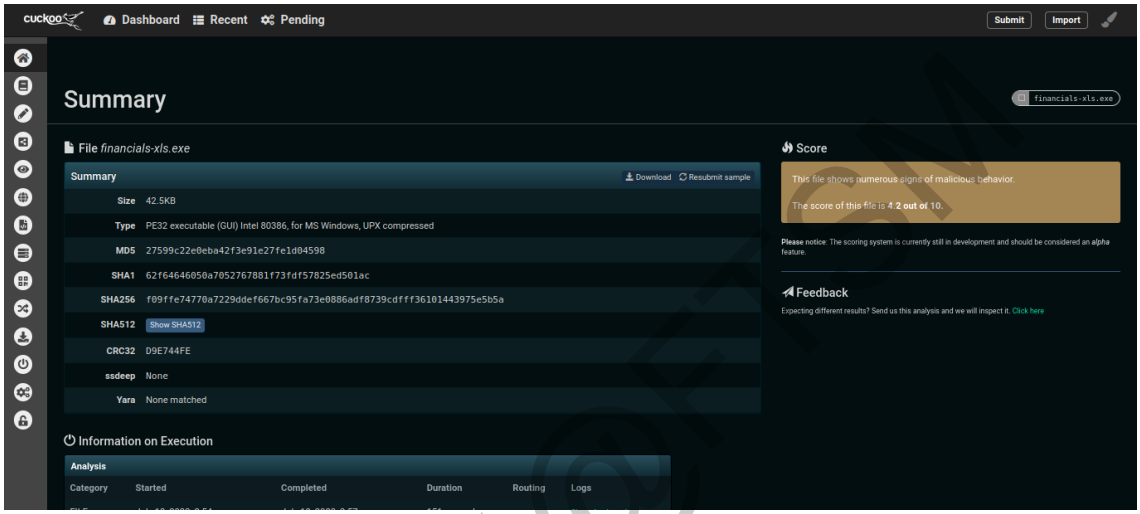
Selepas konfigurasi telah dimuktamadkan, proses analisis akan bermula di mana ia akan menunjuk proses menganalisis dalam halaman yang belum selesai seperti dalam gambar rajah di bawah.



Rajah 6 Halaman Tugasan yang Belum Selesai

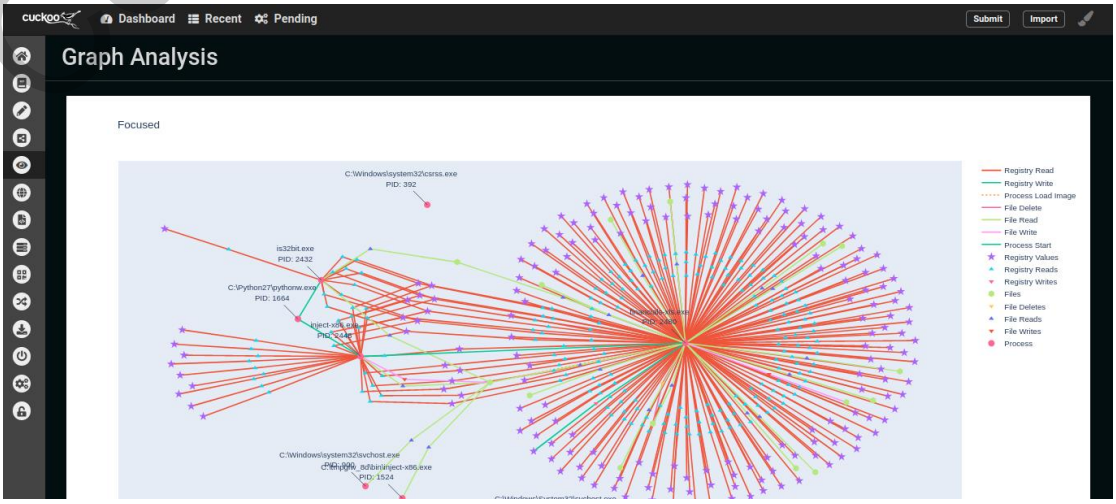
Rajah 7 Proses Fail Dijalankan dalam “VirtualBox”

Setelah analisis telah selesai, sistem akan memaparkan proses telah selesai dan penganalisis boleh menekan pautan “reported” di mana ia akan membawa ke halaman keputusan analisis seperti dalam gambar rajah di bawah.

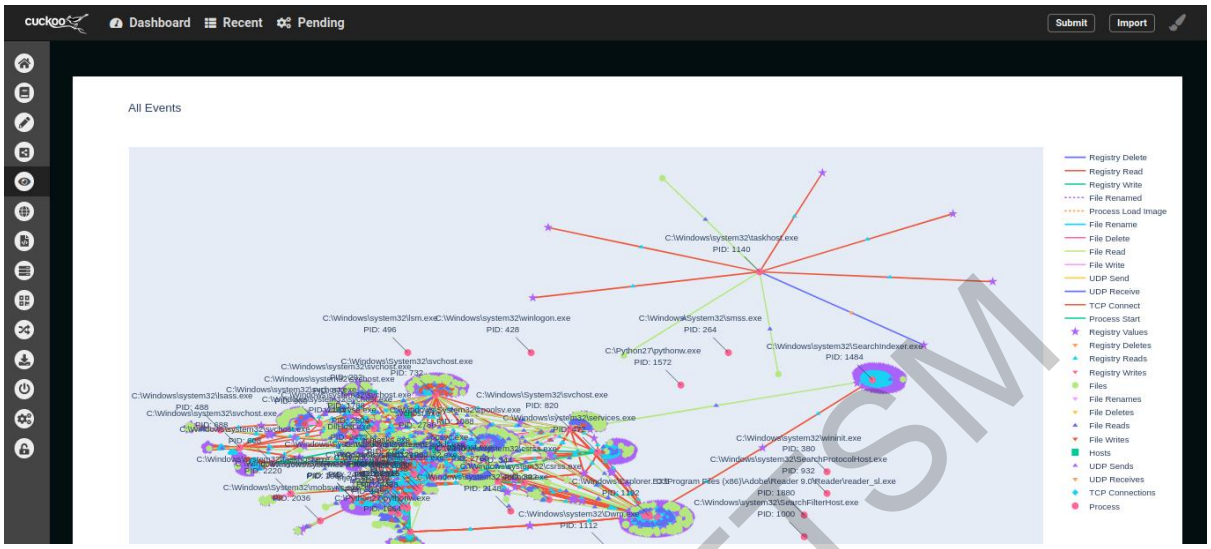


Rajah 8 Halaman Keputusan Ringkasan Fail yang Telah Dianalisis

Penganalisis juga dapat melihat dan berinteraksi dengan graf visualisasi perisian hasad untuk memahami lebih lanjut bagaimana perisian hasad berfungsi ketika ia sedang dilaksanakan.

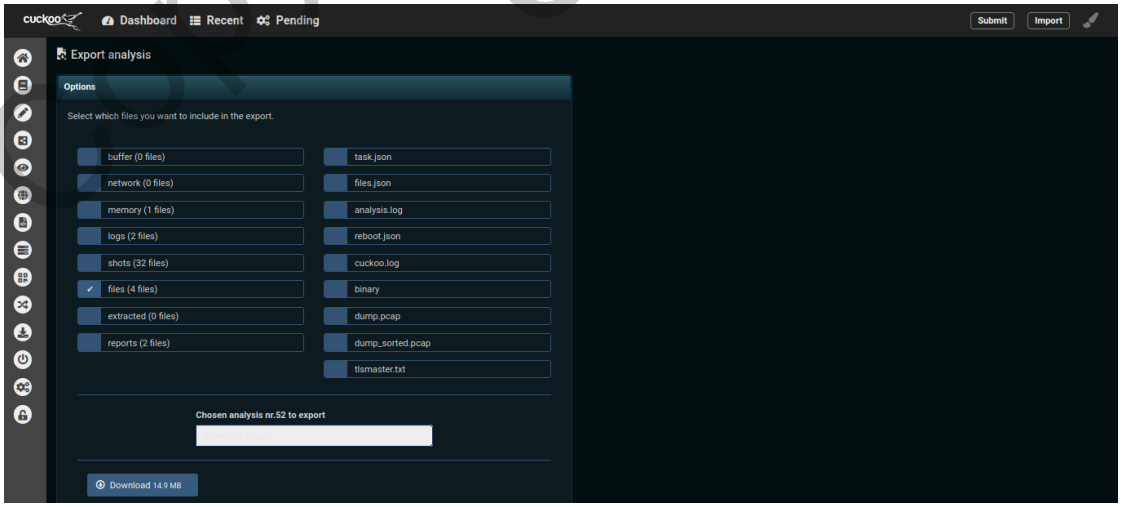


Rajah 9 Halaman Graf Analisis dalam Mod “Focused”

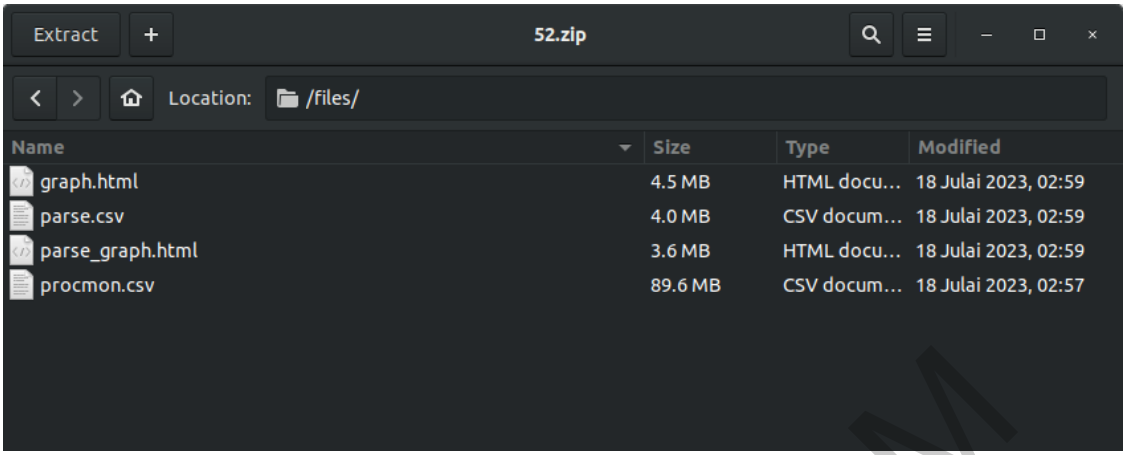


Rajah 10 Halaman Graf Analisis dalam Mod "All Events"

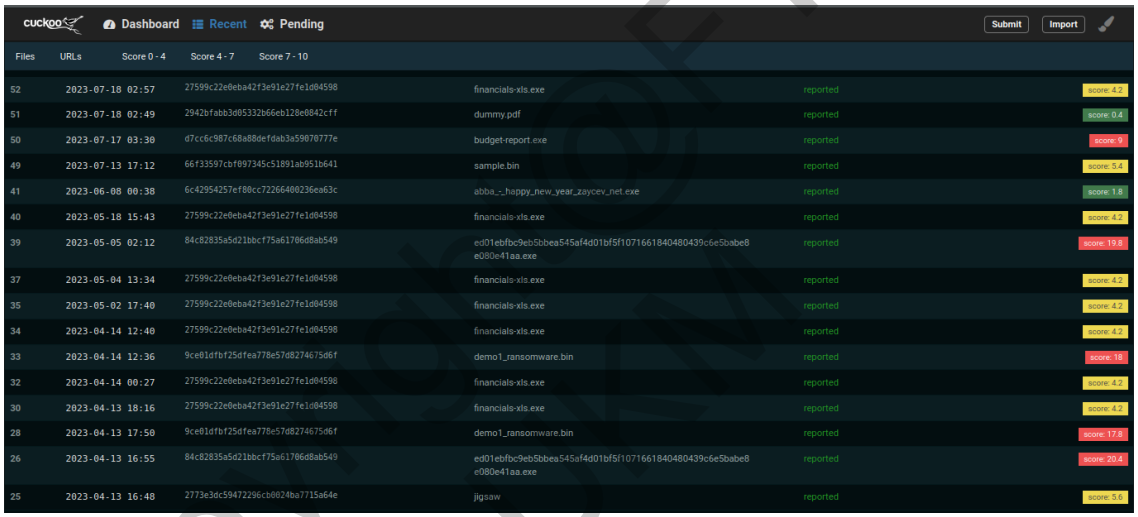
Penganalisis juga boleh mengeksport fail graf dan fail csv procmon jika mereka ingin menggunakan untuk analisis lebih lanjut seperti di gambar rajah 6.8 dan 6.7 di bawah. Mereka juga boleh akses analisis sebelum ini jika mereka mahu melihat keputusan analisis yang telah dijalankan di halaman Analisis Terkini seperti dalam gambar rajah 6.10.



Rajah 11 Halaman Eksport Analisis



Rajah 12 Fail-fail yang Telah Dieksport Ke Dalam Direktori Hos Berbentuk Fail ZIP



Rajah 13 Halaman Analisis Terkini

KESIMPULAN

Kesimpulannya, projek analisis tingkah laku perisian hasad menggunakan visualisasi dengan Cuckoo Sandbox telah terbukti sebagai aset berharga untuk memahami bagaimana perisian berniat jahat berkelakuan. Dengan menggunakan analisis dinamik dan perwakilan visual seperti graf, penganalisis boleh mengenal pasti dan mentafsir corak dan taktik yang digunakan oleh perisian hasad dengan lebih baik. Walau bagaimanapun, penganalisis mesti ingat bahawa keberkesanan sistem mungkin dihadkan oleh versi Python yang lapuk, positif/negatif palsu dan keperluan untuk sampel perisian hasad yang pelbagai. Untuk menambah baik sistem, kemas kini tetap mesti difokuskan dan pengesanan pengelakan yang lebih baik. Dengan peningkatan ini, projek itu akan menyumbang kepada amalan keselamatan siber yang lebih kukuh dan membantu memerangi ancaman yang muncul dengan berkesan. Walaupun terdapat beberapa kekurangan, diharapkan sistem ini dapat dijadikan titik kajian untuk kajian pada masa hadapan.

RUJUKAN

What is cuckoo? What is Cuckoo? - Cuckoo Sandbox v2.0.7 Book. (n.d.). Retrieved April 4, 2023, from https://cuckoo.readthedocs.io/en/latest/introduction/what/

Wikimedia Foundation. (2023, June 26). Knowledge graph. Wikipedia. https://en.wikipedia.org/wiki/Knowledge_graph

Slandau. (2022, February 23). 10 most dangerous new malware and security threats in 2022. CyberTalk. Retrieved November 20, 2022, from https://www.cybertalk.org/2022/02/15/10-of-the-most-dangerous-malware-threats/

Gmcdouga. (2022, February 15). January 2022's most wanted malware: Lokibot returns to the index and Emotet regains top spot. Check Point Software. Retrieved November 20, 2022, from https://blog.checkpoint.com/2022/02/08/january-2022s-most-wanted-malware-lokibot-returns-to-the-index-and-emotet-regains-top-spot/

Wolf, A. (2022, October 25). Most common malware. Arctic Wolf. Retrieved December 4, 2022, from https://arcticwolf.com/resources/blog/8-types-of-malware/

Prayudi, Y. Riadi, I (April 2015). Implementation of Malware Analysis using Static and Dynamic Analysis Method. International Journal of Computer Applications (0975 – 8887).

Efe, A. Salleh, H. (March 2020). Malware Visualization Techniques. International Journal of Applied Mathematics Electronics And Computers 8(1): 007-020, 2020.

Wojner, C. (n.d.). Procdot Online Documentation. PROCDOT's home - online documentation. https://www.procdot.com/onlinedocumentation.htm

Luqman Hariz bin Mat Barhan (A180527)
Wan Fariza Fauzi
Fakulti Teknologi & Sains Maklumat,
Universiti Kebangsaan Malaysia