PLATFORM PENGESANAN PERISIAN HASAD UNTUK SISTEM OPERASI WINDOWS BERDASARKAN KOTAK PASIR, MEMORI ANALISIS DAN FUZZY HASHING

AKMAL HAZIM BIN SURANI

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Penemuan dan perkembangan perisian hasad memang telah menjadi satu cabaran besar dalam dunia siber. Gelombang ransomware dan serangan perisian hasad lainnya telah menunjukkan betapa seriusnya ancaman ini terhadap individu, perniagaan, perkhidmatan awam, dan agensi keselamatan. Oleh itu, analisis perisian hasad menjadi semakin penting untuk mengidentifikasi tingkah laku dan niat perisian hasad, serta untuk mengembangkan teknik pengesanan dan penyingkiran yang berkesan.Tujuan penyelidikan ini adalah untuk menyediakan teknik analisis hibrid yang lebih efisien bagi data perisian hasad dengan menggabungkan analisis tingkah laku dan analisis memori. Dengan cara ini, diharapkan ciri-ciri perisian hasad yang lebih berguna dapat diekstrak dengan lebih baik. Keberkesanan teknik ini akan membantu melindungi institusi dan orang awam daripada serangan perisian hasad dengan mengenal pasti ancaman secepat mungkin sebelum tindakan berbahaya dijalankan.

1 PENGENALAN

Perisian hasad, yang juga dikenali sebagai perisian jahat, merangkumi satu set arahan atau perintah yang dilaksanakan pada sistem komputer untuk mencapai matlamat yang diingini oleh penceroboh (Skoudis & Zeltser, 2004). Mengikut laporan penyelidikan keselamatan siber oleh Positive Technologies tentang Ancaman Lanskap bagi suku pertama tahun 2021 (Q1 2021), serangan siber telah meningkat sebanyak 17% berbanding dengan Q1 2020, dengan peningkatan sebanyak 1.2% dari Q4 2020. Khususnya, 77% daripada serangan-serangan ini dikategorikan sebagai 'serangan bergerak sasaran' (targeted attacks), yang disesuaikan khas untuk individu, kumpulan, laman web, atau perkhidmatan tertentu (Security Magazine, 2021). Serangan bergerak sasaran ini kerap menggunakan kaedah serupa seperti ancaman dalam talian tradisional seperti penghantaran perisian hasad melalui e-mel atau laman web.

Kertas penyelidikan ini mencadangkan satu platform untuk pengesanan perisian hasad yang menggabungkan Cuckoo Sandbox, analisis memori, dan 'fuzzy hashing' (SSDEEP). Analisis memori dipilih untuk mengatasi kelemahan analisis statik dan dinamik. Ini kerana analisis memori adalah cara terbaik untuk mengesan aktiviti berbahaya dalam sistem kerana 'volatile memory' mengekalkan kandungannya selagi sistem tidak dimatikan sepenuhnya. Selain itu, analisis memori juga dapat mengesan perisian hasad dengan cangkuk dan kod yang berfungsi di luar skop fungsi biasa. Maklumat penting seperti sistem operasi, proses yang

berjalan, dan keadaan keseluruhan komputer juga boleh diekstrak melalui analisis memori, menjadikannya teknik analisis yang berkuasa dan berkesan dalam memeriksa tingkah laku perisian hasad

2 PENYATAAN MASALAH

Dalam analisis statik, fail berbahaya dikaji tanpa dijalankan dan ciri-ciri yang diperlukan diekstrak secara tepat. Pendekatan tandatangan digunakan untuk mengenal pasti perisian hasad. Namun, perisian hasad yang baru menggunakan teknik pengeliruan, seperti memasukkan kod mati, mengubah penugasan daftar, menggantikan arahan, dan memanipulasi kod untuk mengelakkan pengesanan analisis statik (Y. Dai, H. Li, Y. Qian, dan X. Lu, 2018). Ini menyebabkan kaedah analisis ini tidak efektif terhadap perisian hasad yang mengubah tandatangan dan mudah dikalahkan oleh perisian hasad. Sebaliknya, Analisis Dinamik melaksanakan dan memantau fail berbahaya dalam persekitaran terkawal. Berbeza dengan analisis statik, analisis tingkah laku tidak terdedah kepada teknik pengeliruan, tetapi ia menggunakan masa dan sumber yang banyak. Perisian hasad yang pintar mungkin mengambil tindakan yang berbeza jika berada dalam persekitaran analisis, seperti berperilaku normal, menamatkan diri, atau berubah menjadi mod tidur.

3 OBJEKTIF KAJIAN

Plaform pengesanan perisian hasad berdasarkan kotak pasir, analisis memori dan fuzzy hashing telah diusul untuk mencapai beberapa objektif seperti Melakukan pemfailan (dump) fail-fail memori Membandingkan fuzzy hashing menggunakan ssdeep dengan menggunakan 2 fail pemfailan (dump) memori.

4 METOD KAJIAN

Kajian ini dibangunkan menggunakan Model Air Terjun yang mudah untuk difahami dan digunakan. Dengan menggunakan kaedah ini, setiap fasa harus dilengkapkan sebelum fasa seterusnya dimulakan. Di penghujung setiap fasa, penilaian dibuat bagi memastikan projek berjalan seperti yang dirancang.

4.1 Fasa Perancangan

Fasa pertama melibatkan merancang dan menentukan matlamat serta skop projek secara terperinci. Pengumpulan keperluan dan kehendak pengguna juga dilakukan pada peringkat ini untuk memahami keperluan platform pengesanan perisian hasad.

4.2 Fasa Analisis

Pada fasa ini, analisis terperinci terhadap keperluan dan kehendak dilakukan. Objektifnya adalah untuk memahami sepenuhnya keperluan perisian hasad dan menyusunnya dalam dokumen analisis yang menyeluruh.

4.3 Fasa Reka Bentuk

Reka bentuk platform pengesanan perisian hasad dilakukan berdasarkan analisis yang telah disiapkan. Selain itu, arsitektur sistem, struktur pangkalan data, dan antaramuka pengguna juga dirancang pada peringkat ini.

4.4 Fasa Implementasi

Di fasa ini, platform pengesanan perisian hasad direalisasikan berdasarkan reka bentuk yang telah disetujui. Perisian hasad dan algoritma 'fuzzy hashing' menggunakan SSDEEP akan diimplementasikan dalam platform ini.

4.5 Fasa Pengujian

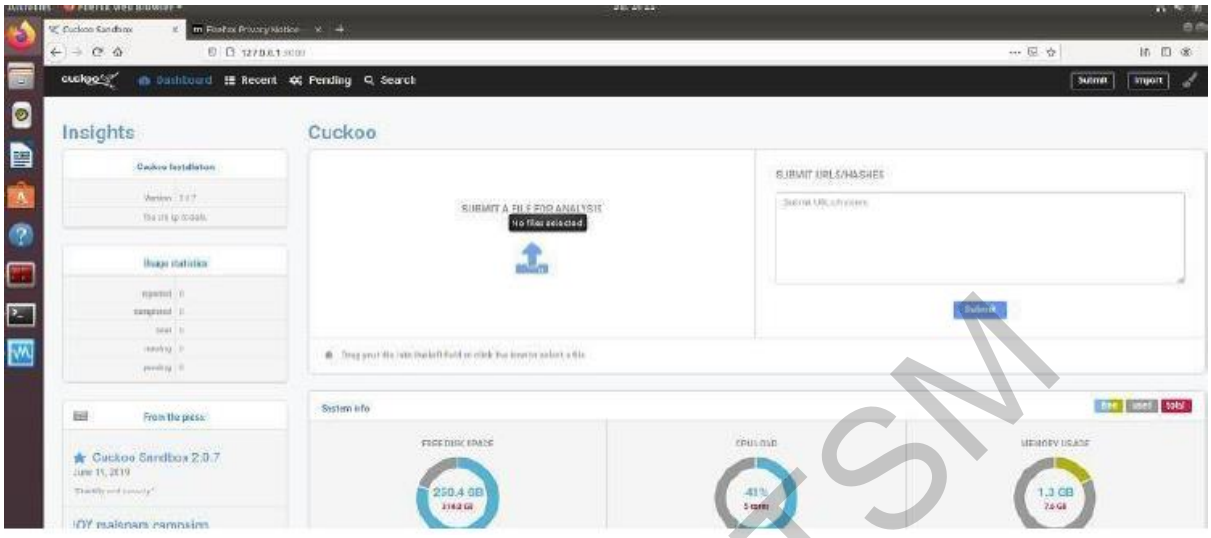
Setelah platform dibangunkan, ujian kesahihan dan kecekapan akan dilakukan untuk memastikan platform berfungsi dengan baik dan memenuhi matlamat projek. Ujian keselamatan dan pengesanan perisian hasad juga akan dijalankan dalam fasa ini.

5 HASIL KAJIAN

Berdasarkan proses pembangunan platform pengesanan perisian ini, terdapat peringkat pengaturcaraan dan langkah-langkah untuk memuat naik platform Cuckoo Sandbox operasi Windows. Syarat-syarat untuk memuat naik Cuckoo Sandbox adalah menyediakan hos, menyediakan tetamu dan memuat naik Cuckoo.Berikut adalah cara-cara untuk memuat naik Cuckoo di Ubuntu menggunakan operasi Windows sebagai “Virtual Machine”.

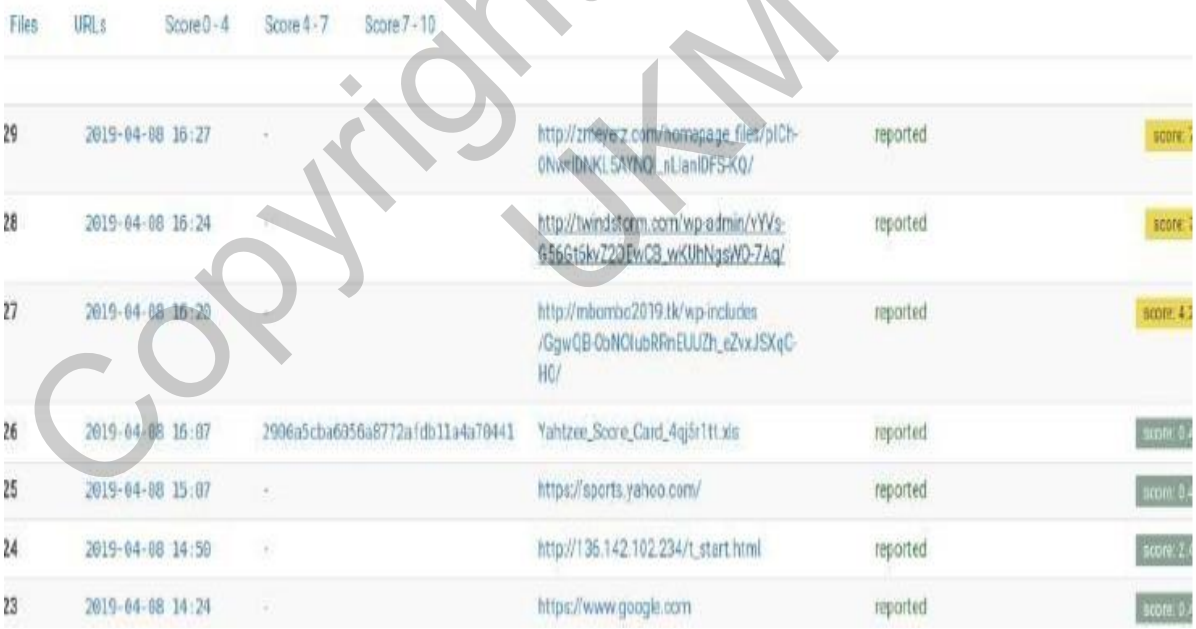
Antara Muka Pengguna

SistemFront-End



Antara Muka Web menyediakan antara muka hadapan yang mesra pengguna untuk berinteraksi dengan Cuckoo Sandbox. Ia membolehkan pengguna menghantar sampel malware, melihat dan menganalisis laporan, serta mengurus proses analisis.

Back-End



Pangkalan data digunakan untuk menyimpan hasil analisis yang dikumpulkan, metadata, dan maklumat tentang sampel malware yang dianalisis. Ia memudahkan untuk mencari semula dan menyoal laporan analisis sebelum ini.

Cuckoo Sandbox memerlukan platform pengevirtualan untuk menjalankan dan menganalisis sampel malware dalam persekitaran yang dikawal.

6 KESIMPULAN

Secara keseluruhannya, Sistem pengesanan perisian hasad ini berjaya dibangunkan walaupun terdapat sedikit masalah pengkompilan kod aturcara. Sistem ini akan dapat membantu Analisa perisian hasad yang memerlukan sistem yang lebih mesra pengguna berbanding sistem yang sedia ada. Walaupun terdapat beberapa kekurangan, diharapkan sistem ini dapat dijadikan titik kajian untuk kajian pada masa hadapan.

7 RUJUKAN

Ed Skoudis dan Lenny Zeltser, Malware: Fighting Malicious Code, New Jersey: Prentice Hall, 2004.

Cyberattacks increased 17% in Q1 of 2020, with 77% being targeted attacks. (2021, July 16). Security Magazine | The business magazine for security executives.

Targeted attacks. (n.d.). Trend Micro | Enterprise Cybersecurity Solutions. What is malware and how does it work? (2020, November 3). SearchSecurity.

What is a malware file signature (And how does it work)? (2021, October 6). SentinelOne.

Shiel, Ian & O'Shaughnessy, Stephen. (2019). Improving file-level fuzzy hashes for malware variant classification. Digital Investigation. 28. S88-S94. 10.1016/j.diin.2019.01.018.

Ye, Y.; Li, T.; Adjeroh, D.; Iyengar, S.S. A Survey on Malware Detection Using Data Mining Techniques. ACM Comput. Surv. 2017, 50, 41