MEMBANGUN SISTEM DETEKSI *MALWARE* MENGGUNAKAN MALICE PADA SISTEM OPERASI BERBASIS LINUX

Muhammad Nur Maajid[1], Mochammad Fahru Rizal[1], Setia Juli Irza Ismail[2]

[1,2,3] Universitas Telkom, Bandung
muhammadnurmaajid@student.telkomuniversity.ac.id[1], mfrizal@telkomuniversity.ac.id[2], julismail@telkomuniversity.ac.id[3]

Abstrak

lebih dari 1,500 perusahaan di Amerika mengalami serangan ransomware, serangan tersebut terjadi pada hari jumat, memungkinkan para peretas melumpuhkan ratusan bisnis di lima benua. Sebagian besar kantor dokter gigi dan kantor akuntan mengalami gangguan, gangguan lebih terasa di Swedia dimana ratusan supermarket harus tutup karena mesin kasir mereka tidak berfungsi. Malware adalah perangkat lunak yang dibuat untuk tujuan jahat, karena mengganggu kinerja sistem komputer. Malware memasuki sistem dan melakukan eksploitasi. Karena malware terus berkembang, salah satu upaya yang bisa dilakukan adalah mengimplementasikan MALICE untuk menganalisis malware. MALICE adalah framework yang memfasilitasi analisis malware dengan menjalankan plugin MALICE melakukan yang terbaik untuk menentukan modul pemrosesan mana yang harus dijalankan selama setiap analisis, dan menjalankan eksekusi modul rantai untuk mencapai analisis end-to-end. Pada proyek akhir ini dibangun sistem analisis *malware* menggunakan MALICE untuk menghindari serangan *malware*. Dari hasil pengujian, sistem ini berhasil menunjukan informasi dasar objek *malware*, informasi ini berguna untuk dilaporkan kepada pengembang antivirus sebagai bahan acuan untuk memperbarui signature antivirus ke depannya.

Kata kunci: Malware, Malice, Analisa Malware, Sistem Analisis

Abstract

More than 1,500 U.S. companies suffered ransomware attacks, the attack took place on Friday, allowing hackers to cripple hundreds of businesses on five continents. Most dentist's offices and accounting firms are experiencing disruptions, a disruption more pronounced in Sweden where hundreds of supermarkets have had to close because their cash registers are not working. Malware is software created for malicious purposes, as it interferes with the performance of a computer system. Malware enters the system and exploits. As malware continues to grow, one of the efforts that can be done is to implement MALICE to analyze malware. MALICE is a framework that facilitates malware analysis by running malice plugins doing their best to determine which processing modules should run during each analysis, and executing chain modules to achieve end-to-end analysis. In this final project built a malware analysis system using MALICE to avoid malware attacks. From the results of the test, this system managed to show the basic information of malware objects, this information is useful to report to antivirus developers as a reference material to update antivirus signatures in the future.

Keyword : Malware, Malice, Malware Analysis, Analysis System

1. Pendahuluan

Dengan ditemukannya teknologi-teknologi baru maka perkembangan teknologi informasi saat ini menjadi tidak terelakkan, teknologi tersebut sebenarnya dirancang untuk membantu kehidupan masyarakat sehari-hari. Internet adalah jaringan komputer besar yang saling berhubungan yang dapat menghubungkan orang dan komputer di seluruh dunia. Untuk memungkinkan orang bertukar informasi dan data, sejumlah besar aktivitas Internet membuat pengguna Internet rentan terhadap serangan *malware*. Selain banyaknya penggunaan internet, *malware* semakin banyak memasuki komputer melalui perantara *file*. *Malware* adalah perangkat lunak yang dibuat untuk tujuan jahat dan berbahaya karena dapat mengganggu kerja sistem komputer. *Malware* memasuki sistem dan menggunakannya tanpa izin, seperti merusak data, perangkat, atau orang.

Dilansir dari reuters.com lebih dari 1,500 perusahaan di Amerika mengelami serangan ransomware yang terjadi di U.S. [1] menunjukkan semakin berkembangnya *malware* dengan cepat. Oleh karena itu, diperlukan teknologi baru yang dapat menganalisis perangkat lunak berbahaya untuk mendeteksi perangkat lunak berbahaya yang memasuki komputer. Diperlukan penggunaan sistem yang kompleks untuk analisis *malware* dan penggunaan beberapa fungsi dalam satu sistem. MALICE adalah salah satu *framework* yang dibuat untuk melakukan analisis *malware* dengan menjalankan plugin dan menentukan modul pemrosesan mana yang harus dijalankan selama setiap analisis dan menjalankan modul untuk mencapai analisis *end-to-end*.

Saat melakukan analisis *malware*, maka akan diperoleh informasi dasar tentang sampel *malware* tersebut. Informasi sampel *malware* tersebut dianalisis dengan berbagai cara, salah satunya dengan mengekstrak stringnya. Ekstraksi string adalah sepotong teks yang menampilkan informasi *file* penyusun objek. Selama proses ekstraksi ini, informasi tentang *malware* dapat diperoleh. Penelitian ini menggunakan MALICE untuk membuat sistem analisis *malware*. Keuntungan dari sistem analisis *malware* ini adalah dapat menampilkan beberapa informasi. Informasi ini dibutuhkan untuk mempelajari *malware* dan diharapkan dapat membantu menemukan *malware* secara lebih detail, sehingga didapatkan hasil yang dapat diberikan kepada pengembang antivirus sebagai hasil pembuatan materi antivirus. Sistem akan dibangun pada ruang lingkup virtual mesin

2. Dasar Teori

a. Sistem Analisis

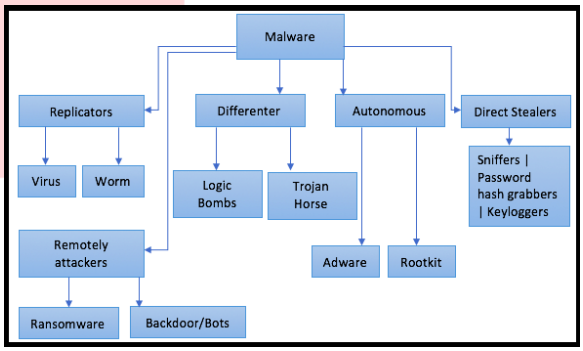
Merupakan upaya mengamati sesuatu detail dengan cara menguraikan komponen pembentuknya untuk dikaji lebih lanjut.[2]

b. Analisis Malware

Merupakan proses membedah komponen – komponen *malware* dan mempelajari tujuan fungsi *malware* tertentu. Proses ini dapat mengetahui jenis *malware*.[3]

c. Malware

Malware atau *Malicious Software* merupakan sebuah program atau *software* jahat yang sengaja dibuat dengan tujuan memasuki dan merusak sistem komputer, jaringan atau server tanpa diketahui oleh pemiliknya. *Malware* biasanya disusupkan kedalam jaringan internet. Jika disusupkan secara manual ke dalam komputer korban tentu saja akan sangat sulit. Jadi kebanyakan peretas melakukan aksinya menggunakan bantuan jaringan internet.[4] [5]



d. Malice

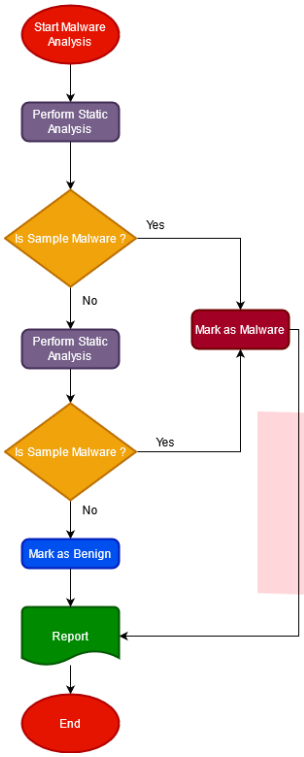
Malice adalah platform analisis malware terbuka yang dibangun untuk memfasilitasi analisis file yang terkait perangkat lunak perusak atau malware.[6] [7]

e. VirtualBox

VirtualBox adalah program untuk virtualisasi komputer yang ditujukan untuk komputer desktop, server dan *embedded system*. Dengan menggunakan virtualbox dapat mem-virtualisasi OS (*Operating System*) 32 bit dan 64 bit pada sebuah komputer yang menggunakan prosesor Intel atau AMD, baik virtualisasi *software* maupun *hardware.*

3. Analisis dan Perancangan Sistem

a. *Flowchart* Sistem



Gambar 1 Flowchart Sistem

Sistem yang akan dibangun terdiri dari satu mesin fisik yaitu sebuah *laptop* yang bertugas sebagai *host* analisis dan mengelola sampel *malware*. Laporan hasil analisis *malware* di proses oleh *host* kedalam bentuk laporan analisis. Akses internet dibutuhkan untuk memanggil API VirusTotal untuk memeriksa *signature file* yang dianalisis.

4. Hasil dan Pembahasan

Analisis dilakukan dengan Malice, VirusTotal dan analisis statis.

a. Sampel Analisis

Sampel yang akan diujikan untuk melakukan analisis malware sebagai berikut.

No	Nama Sampel	Index Sampel	Kategori Sampel
1	Mssecsvc.bin	1	Malware
2	Test.txt	2	Belum Diketahui
3	Test2.txt	3	Belum Diketahui
4	Trickbot.bin	4	Malware
5	Trojan.bin	5	Malware
6	Dropper.bin	6	Malware
7	Eternal.bin	7	Malware
8	GenTro.tmp	8	Malware
9	NewGenTro.bin	9	Malware
10	sdBot.bin	10	Malware

Keterangan Sampel:

Mssecsvc.bin, Trickbot.bin, Trojan.bin, Dropper.bin, Eternal.bin, GenTro.tmp, NewGenTro.bin dan sdBot.bin Sampel ini diambil dari github yang positif terdeteksi sebagai *malware*.

Test.txt dan test2.txt Sampel ini diambil dari komputer pribadi, belum dapat dipastikan sampel termasuk *malware* atau bukan.

b. Pengujian Malice dan VirusTotal

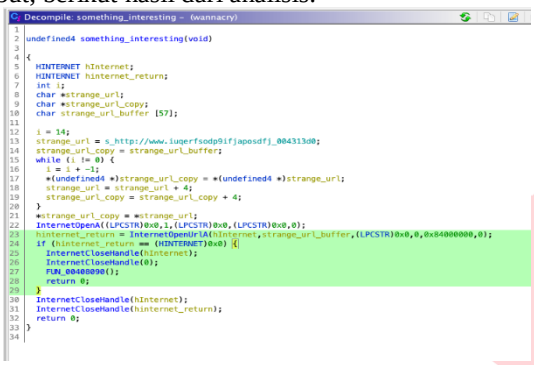
Tujuan dari pengujian ini adalah membandingkan Malice ratio dengan Virustotal ratio untuk mengetahui kelebihan dan kekurangan dari Malice.

No	Nama Sampel	Malice Ratio dan VirusTotal Ratio	Jenis Malware
1	Mssecsvc.bin	11% dan 57%	Ransomware
2	Test.txt	0%	Bukan Malware
3	Test2.txt	0%	Bukan Malware
4	Trickbot.bin	6% dan 57%	RAT
5	Trojan.bin	5% dan 62%	Trojan
6	Dropper.bin	0% dan 62%	RAT
7	Eternal.bin	5% dan 59%	BOTS
8	GenTro.tmp	0% dan 3%	Trojan
9	NewGenTro.bin	0% dan 56%	Trojan
10	sdBot.bin	6% dan 61%	Ransomware

Berdasarkan pengujian tabel dapat disimpulkan bahwa Malice pada sampel no 6, 8, dan 9 tidak dapat mendeteksi sampel sebagai malware dikarenakan tidak ada signature untuk malware yang diuji.[8]

c. Pengujian Analisis Manual

Untuk pengujian analisis manual menggunakan ghidra, ghidra adalah perangkat lunak *open source* yang digunakan untuk melakukan analisis *malware* dengan metode *reverse engineering*[9] Teknik membongkar sebuah sistem dari *file* atau aplikasi untuk melihat seluruh data dan informasi dari *file* atau aplikasi tersebut, berikut hasil dari analisis.



Pada baris 23 membuat *request* ke URL, baris 24 jika *request* gagal mengembalikan menjadi null dan memanggil *function* FUN_00408090, jika *request* berhasil maka handle akan tertutup dan keluar dari program.

5. Kesimpulan

Berdasarkan hasil dari pengujian, maka dapat disimpulkan sebagai berikut.

1. MALICE telah berhasil dibangun pada ruang lingkup mesin virtual dengan sistem operasi berbasis Linux.
2. Perbandinga ratio antara malice ratio dan virustotal ratio sangat jauh. Dikarenakan malice masih mengalami beberapa kendala pada plugin antivirus.

Referensi

[1] "Up to 1,500 businesses affected by ransomware attack, U.S. firm's CEO says | Reuters." [Online]. Available: https://www.reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05/. [Accessed: 27-Jul-2021].

[2] "OPSWAT | Malware Analysis." [Online]. Available: https://www.opswat.com/solutions/malware-analysis. [Accessed: 10-May-2021].

[3] D. Distler, "Information Security Reading Room Malware Analysis : An Malware Analysis : An Introduction tu , A ho ll r igh," 2019.

[4] "8 Different Types of Malware | United States Cybersecurity Magazine." [Online]. Available: https://www.uscybersecurity.net/malware/. [Accessed: 10-Apr-2020].

[5] "Apa itu Malware? Pengertian dan Cara Mengatasinya - Niagahoster," 11-Sep-2018. [Online]. Available: https://www.niagahoster.co.id/blog/apa-itu-malware/. [Accessed: 04-May-2020].

[6] "GitHub - maliceio/malice: VirusTotal Wanna Be - Now with 100% more Hipster," 18-Mar-2019. [Online]. Available: https://github.com/maliceio/malice. [Accessed: 13-May-2020].

[7] "Local Malware Analysis with Malice." [Online]. Available: https://isc.sans.edu/forums/diary/Local+Malware+Analysis+with+Malice/25544/. [Accessed: 10-Apr-2020].

[8] "Malware Analysis Explained | Steps & Examples | CrowdStrike." [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/. [Accessed: 10-May-2021].

[9] "Reverse Engineering Malware: Getting Started with Ghidra, Part 1." [Online]. Available: https://www.hackers-arise.com/post/reverse-engineering-malware-getting-started-with-ghidra-part1. [Accessed: 10-Sep-2021].