2. LANDASAN TEORI

2.1 Tinjauan Pustaka

2.1 Malware

Malware adalah perangkat lunak yang diciptakan untuk menyusup atau merusak sistem komputer, server atau jejaring komputer tanpa izin (informed consent) dari pemilik. Malware bisa menyebabkan kerusakan pada sistem komputer dan memungkinkan juga terjadi pencurian data / informasi (EduCSIRT Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi,2021). Hal yang pada umumnya menjadi penyebab malware adalah mengunduh perangkat lunak (software) ilegal yang mungkin disisipkan sebuah malware. Terdapat beberapa jenis Malware seperti virus, worm, trojan horse, sebagian besar rootkit, spyware, adware (infected), serta software-software lain yang berbahaya dan tidak diinginkan oleh pengguna perangkat komputer.

2.1.1 Virus

Virus merupakan perangkat lunak berbahaya yang menggandakan dirinya sendiri dengan menyuntikkan kodenya ke program lain(Karresand,M,2003**)**. Virus dapat menyebar dari satu program ke program lain dan dari satu komputer ke komputer lain.

2.1.2 Worms

Worms menargetkan kerentanan dalam sistem operasi untuk menginstal dirinya sendiri ke dalam jaringan(Gudang SSL,2021). Mereka dapat memperoleh akses dengan beberapa cara: melalui pintu belakang yang terpasang pada perangkat lunak, melalui kerentanan perangkat lunak yang tidak disengaja, atau melalui flash drive. Begitu ada, worm dapat digunakan oleh aktor jahat untuk meluncurkan serangan DDoS, mencuri data sensitif, atau melakukan serangan ransomware.

2.1.3 Trojan Horse

Trojan adalah salah satu jenis malware yang mengancam. Mereka akan berpura-pura menjadi sesuatu yang sah dan kemudian mengepung sistem komputer Anda (NordVPN,2021). Peretas biasanya memanfaatkan berbagai macam teknik rekayasa sosial agar korban dapat dikelabui sehingga mengunduh malware.

2.1.4 Backdoor

Backdoor adalah virus yang memiliki kesamaan dengan trojan, hanya saja virus ini menyerupai program-program yang terlihat biasa-biasa saja, contohnya adalah game. Virus

ini mampu digunakan oleh peretas untuk masuk ke sebuah sistem tanpa harus melakukan autentikasi.(Gudang SSL,2021)

2.1.5 Adware

Adware merupakan perangkat lunak yang didukung iklan adalah jenis malware yang terus-menerus membawa iklan ke komputer. Biasanya adware dibundel dengan perangkat lunak yang diunduh gratis dan aplikasi seperti permainan gratis(Mohammed,Ithnin,2017)

2.1.6 Ransomware

Ransomware adalah perangkat lunak yang menggunakan enkripsi untuk menonaktifkan akses target ke datanya hingga uang tebusan dibayarkan. Organisasi korban dibuat sebagian atau seluruhnya tidak dapat beroperasi sampai membayar, tetapi tidak ada jaminan bahwa pembayaran akan menghasilkan kunci dekripsi yang diperlukan atau bahwa kunci dekripsi yang diberikan akan berfungsi dengan baik. (Crowdstrike,2023)

2.1.7 Fileless Malware

Fileless Malware tidak menginstal apa pun pada awalnya, melainkan membuat perubahan pada file asli sistem operasi, seperti PowerShell atau WMI. Karena sistem operasi mengenali file yang diedit sebagai file yang sah, serangan tanpa file tidak tertangkap oleh perangkat lunak antivirus — dan karena serangan ini diam-diam, serangan ini sepuluh kali lebih berhasil daripada serangan malware tradisional. (Crowdstrike,2023)

2.1.8 Spyware

Spyware adalah perangkat lunak berbahaya yang dirancang untuk mengumpulkan informasi secara diam-diam tentang seseorang atau organisasi tanpa sepengetahuan atau persetujuan mereka. Ini adalah jenis malware (perangkat lunak berbahaya) yang biasanya beroperasi secara diam-diam di latar belakang komputer atau perangkat elektronik lainnya, mengumpulkan data dan mengirimkannya ke pihak ketiga. Spyware sering kali memasuki sistem melalui cara yang menipu, seperti digabungkan dengan perangkat lunak yang tampaknya sah atau disembunyikan di dalam situs web atau lampiran email berbahaya. Untuk melindungi dari spyware, penting untuk memiliki perangkat lunak antivirus dan anti-malware terbaru, berhati-hati dalam mengunduh dan menginstal perangkat lunak dari sumber yang tidak terpercaya, dan menerapkan kebersihan keamanan siber yang baik. (Fortinet,2023)

2.1.9 Dropper

Dropper merupakan jenis perangkat lunak yang berbahaya karena mempunyai tujuan yaitu untuk menginstal, melepaskan, menjalankan perangkat lunak berbahaya lainnya pada sistem host. Dropper biasanya sebagai komponen utama dalam melakukan penyebaran dan kerusakan sistem karena mereka dapat melemah sistem anti virus dari suatu sistem. Mereka juga dapat menyembunyikan malware utama dan menghindari sistem keamanan komputer. (Perception Point,2023)

2.2 Model Analisis Malware

Pada dasarnya malware adalah sebuah program, yang disusun berdasarkan tujuan tertentu dengan menggunakan algoritma yang sudah disesuaikan. Oleh karena
itulah maka model analisis yang biasa dipergunakan untuk mengkaji malware sangat erat kaitannya dengan ilmu dasar komputer, yaitu: bahasa pemrograman, algoritma, struktur data, dan rekayasa piranti lunak. Secara Umum ada beberapa jenis analisa terhadap sebuah program atau malware.

2.2.1 Analisis Malware Statis

Merupakan metode yang digunakan untuk melakukan analisa malware dengan cara mengamati secara langsung kode sumber (source code) malware tersebut. Dalam mengamati kode sumber malware.**(N-Able,2019)** Analisis statis memeriksa file malware tanpa benar-benar menjalankan program. Dalam bentuknya yang paling dasar, analisis statis mengumpulkan informasi dari malware bahkan tanpa melihat kodenya. Metadata seperti nama file, jenis, dan ukuran dapat memberikan petunjuk tentang sifat malware. Checksum atau hash MD5 dapat dibandingkan dengan database untuk menentukan apakah malware telah dikenali sebelumnya. Dan pemindaian dengan perangkat lunak antivirus dapat mengungkapkan malware yang berjalan didalam sistem.**(N-Able,2019)**

Analisis statis tidak memerlukan kode yang sedang berjalan. Sebaliknya, analisis statis memeriksa data untuk tanda-tanda niat jahat. Sangat berguna untuk mengidentifikasi masalah buruk, perpustakaan, atau bahan pengemasan. Memeriksa informasi spesifik seperti nama file, hash, string seperti alamat IP, domain, dan informasi header file yang dapat digunakan untuk menentukan apakah suatu file berbahaya. Selain itu, alat seperti parser dan penganalisa jaringan untuk mengumpulkan informasi tentang cara kerjanya dapat digunakan untuk menganalisis malware tanpa benar-benar menjalankannya.

Namun, karena tidak menjalankan kode analisis statis, malware tingkat lanjut mungkin memiliki perilaku runtime berbahaya yang tidak terdeteksi. Misalnya, jika database membuat larik dan kemudian mengambil data yang tidak valid sebagai larik dinamis, analisis statis tidak akan

mendeteksinya. Perusahaan beralih ke analitik dinamis untuk lebih memahami perilaku data.**(Crowdstrike,2023)**

2.2.2 Analisis Malware Dinamis

Merupakan metode yang digunakan untuk melakukan analisa terhadap malware dengan mengamati kinerja sistem yang dapat terlihat dari perilaku sistem sebelum malware dijalankan dengan perilaku sistem setelah malware tersebut dijalankan pada sistem tersebut. Metode dynamic analysis umumnya menggunakan software virtual seperti VirtualBox, VMWare dan lain-lain, sehingga apabila malware yang dijalankan tersebut ternyata merusak sistem, maka sistem utama tidak mengalami kerusakan akibat malware tersebut.**(N-Able,2019)**

Analisis malware dinamis mengeksekusi kode berbahaya yang dicurigai di lingkungan aman yang disebut *sandbox*. Sistem tertutup ini memungkinkan profesional keamanan untuk memantau aksi malware tanpa risiko menginfeksi atau memasuki jaringan perusahaan. Analisis Dinamis memberikan visibilitas yang lebih dalam kepada pemburu ancaman dan tim tanggap insiden terhadap sifat sebenarnya dari ancaman tersebut. Keuntungan kedua adalah kotak pasir otomatis menghilangkan waktu yang diperlukan untuk merekayasa balik data untuk menemukan kode berbahaya.Kesulitan dengan analisis dinamis adalah jika malware cukup canggih, mereka tahu *sandbox* itu ada dan karenanya sangat pandai mendeteksinya. Untuk mengeksploitasi *sandbox*, penyerang menyembunyikan kode di dalamnya yang akan tetap aktif hingga kondisi tertentu terpenuhi. Hanya dengan begitu kode akan berfungsi.**(Crowdstrike,2023)**

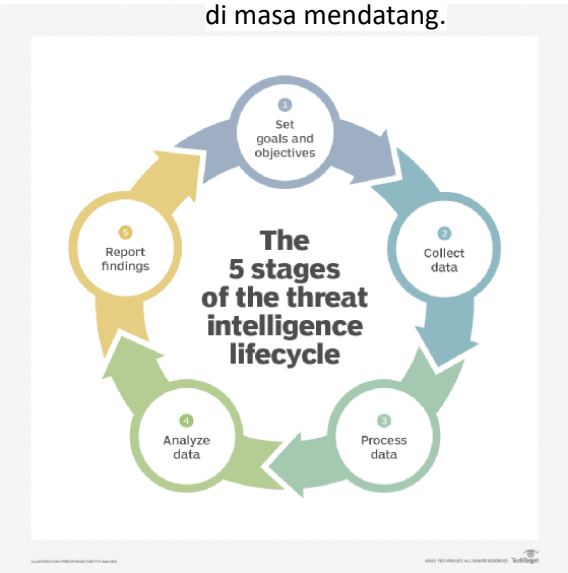
2.3 Threat Intelligence

Threat Intelligence adalah proses mengidentifikasi dan menganalisis ancaman dunia maya. Istilah '*Threat Intelligence*' dapat merujuk pada data yang dikumpulkan tentang potensi ancaman atau proses pengumpulan, pemrosesan, dan analisis data tersebut untuk memahami ancaman dengan lebih baik. Kecerdasan ancaman melibatkan penyaringan data, memeriksanya secara kontekstual untuk menemukan masalah dan menyebarkan solusi khusus untuk masalah yang ditemukan **(Kaspersky,2023)**

Threat Intelligence adalah bagian penting dari setiap ekosistem keamanan siber. Dengan adanya data dari Threat Intelligence, dapat:

- Cegah kehilangan data: Dengan data analisis yang terstruktur dengan baik, organisasi dapat menemukan ancaman dunia maya dan mencegah pembobolan data agar tidak merilis informasi sensitif.

- Memberikan arahan tentang langkah-langkah keamanan: Dengan mengidentifikasi dan menganalisis ancaman, CTI melihat pola yang digunakan peretas dan membantu organisasi menerapkan langkah-langkah keamanan untuk melindungi dari serangan di masa mendatang.



Gambar 2.1 Threat Intelligence

Sumber : https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.techtarget.com%2Fwhatis%2Fdefinition%2Fthreat-intelligence-cyber-threat-intelligence&psig=AOvVaw1ogMiP4Dt9r4g3M0CQQI8P&ust=1700230011284000&source=images&cd=vfe&opi=89978449&ved=0CBEQjRxqFwoTCKCM9LzYyIIDFQAAAAAdAAAAABAE

2.4 Tinjauan Studi

A) **A survey on malware detection and analysis tools. Talukder. (2020).** Penelitian ini membahas tentang tools analisa malware yang digunakan untuk analisa statis dan dinamis. Hubungan dengan penelitian ini adalah kesepahaman dalam konsep metode static analysis untuk melakukan analisa malware, sedangkan perbedaan dengan penelitian ini adalah tools yang digunakan tidak semua dipakai.

B) **GandCrab Ransomware Analysis on Windows using Static Method (Anisa Oktaviani, Melwin Syafrizal)**.Penelitian ini membahas tentang analisa malware ransomware menggunakan metode static analysis. Hubungan dengan penelitian ini adalah kesepahaman konsep tentang metode static analysis, sedangkan perbedaan dengan penelitian ini adalah aplikasi yang terduga malware telah diketahui karakteristik malware ransomware.

C) **Separating Trojan Horses, viruses, and worms (Karresand, M)**. penelitian ini membahas mengenai perbedaan dari jenis jenis malware yang ada. Persamaan dari penelitian ini adalah jenis malware yang digunakan akan sama namun perbedaan nya malware yang digunakan akan dilakukan analisis dan penelitian lebih lanjut untuk mendapatkan hasil yang lebih detail.

D) **Analysis of Malware methods using dynamic analysis in detecting malware. (Situmorang, Sutrisno, Harmoko Lubis, Jontinus Manullang)** . Penelitian ini melakukan pengujian tools menggunakan metode analisis dinamis, persamaan dengan penelitian ini yaitu metode yang digunakan dalam analisis. Sedangkan perbedaan penelitian yaitu dalam segi tools dan malware yang akan dianalisis.

E) **A Survey on Malware Analysis Techniques: Static, Dynamic, Hybrid and Memory Analysis**. Dalam paper ini membahas teknik dalam melakukan analisis malware dengan beberapa cara mulai dari static hingga memory analysis. Hubungan dengan penelitian ini adalah kesamaan konsep dalam penggunaan metode dalam melakukan analisis yaitu menggunakan static dan dynamic malware analysis.

2.5 Referensi Perbandingan Penelitian Sejenis

Tabel 2.1
Tabel Perbandingan penelitian

Penelitian Sebelumnya	**Penelitian Sekarang**
Menggunakan satu metode dalam melakukan Analisis	**Menggunakan Dua metode dalam melakukan Analisis**
Malware yang di analisis hanya trojan	**Malware yang dianalisis lebih beragam**
Penelitian dilakukan untuk mengumpulkan informasi mengenai trojan	**Penelitian dilakukan untuk mempelajari cara kerja malware dan kinerja dari kedua metode dalam melakukan analisis**
Hasil Penelitian digunakan untuk mengetahui cara kerja analisis tertentu	**Hasil Penelitian diimplementasikan dalam bentuk buku panduan untuk PTIK**