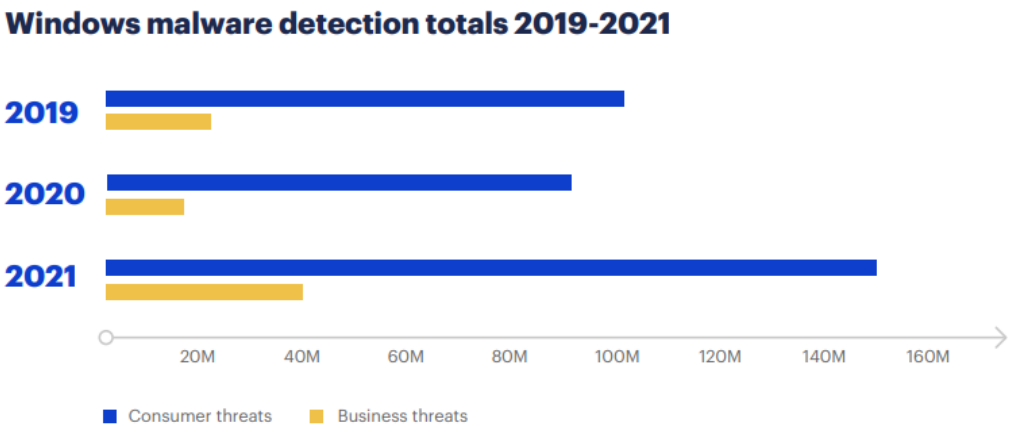
BAB 1
PENDAHULUAN

1.1 Latar Belakang

Teknologi telah ada sejak dahulu kala dan masih terus berkembang. Pesatnya perkembangan teknologi didorong oleh kebutuhan manusia yang semakin beragam bentuknya. Teknologi erat kaitannya dengan individu dan organisasi dan penerapannya memberikan kemudahan dalam berbagai situasi. Salah satu teknologi yang berkembang pesat saat ini adalah *Internet*. *Internet* sendiri telah menjadi bagian penting dari kehidupan kita sehari – hari untuk kegiatan di bidang industri, pendidikan dan lainnya.

Keberadaan *Internet* sangat bermanfaat bagi kehidupan manusia. Dengan adanya *Internet*, manusia diberi kemudahan untuk menjalankan aktivitas sehari – hari khususnya di bidang industri. Dalam bidang industri, *internet* diperlukan untuk saling bertukar informasi secara cepat. Kemudahan ini memunculkan pula berbagai celah keamanan yang seringkali dimanfaatkan oleh orang yang tidak bertanggung jawab. Dengan mengambil informasi tersebut, pelaku dapat mendapatkan keuntungan dari korban. Pencurian informasi oleh orang yang tidak bertanggung jawab ini dapat dilakukan dengan berbagai teknik dan salah satunya adalah *Malware (Malicious Software).*

Penyebaran *Malware* di Indonesia sendiri pada kuartal 1 mencapai persentase 44% di tahun 2019 (Virgiawan A. Manoppo, Arie S. M. Lumenta, 2020). *Trojan, Virus, Spyware* dan *Exploit* merupakan beberapa contoh dari *Malware* yang masing – masing memiliki karakteristik yang berbeda (Virgiawan A. Manoppo, Arie S. M. Lumenta, 2020). Berdasarkan (MalwareBytes cyberprotection, 2022), sistem operasi Windows sendiri dari tahun 2019 ke 2020 mengalami penurunan untuk serangan *malware* dan kembali melonjak ketika pandemi Covid-19 di tahun 2021 dan untuk lebih jelasnya dapat dilihat pada gambar 1.1. Kenaikan yang cukup signifikan ini mencapai persentase 300%.



Gambar 1. 1 Windows Malware Detection 2019 - 2021 dikutip dari sumber: (MalwareBytes cyberprotection, 2022)

SIEM mampu untuk melakukan pengumpulan *log* dari *event* yang sedang berlangsung melalui *open source* sehingga seluruh sistem mendapat pengawasan langsung.

Penulis pada penelitian ini akan menggunakan *tool open source* bernama Wazuh. Alasan penulis menggunakan Wazuh karena memiliki fitur yang cukup lengkap dan terlebih merupakan aplikasi *open source* atau gratis. SIEM dapat diaplikasikan melalui Wazuh yang akan melakukan pengumpulan data hingga deteksi ancaman. Selain itu, penulis tidak akan menggunakan sistem operasi Windows, melainkan Debian untuk pengujiannya. Hal ini karena sistem operasi berbasis Linux sifatnya *open source* sehingga apabila terdapat *bug* atau *crash*, semua orang yang menggunakan sistem operasi tersebut dapat berkontribusi untuk melaporkan hal tersebut kepada *developer*. Sedangkan Windows merupakan sistem operasi yang *closed source* yang harus menunggu *developer* untuk memperbaikinya dan biasanya harus ada kejadian besar yang merugikan.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dijelaskan sebelumnya, maka identifikasi masalah adalah sebagai berikut:

1. Seringnya terjadi serangan *Malware* (*malicious software)* terhadap suatu perangkat komputer individu maupun organisasi.

2. *File* yang baru diunduh tidak diketahui karakteristiknya dan bisa saja berupa *malware* yang berbahaya untuk suatu perangkat komputer.

1.3 Rumusan Masalah

Berdasarkan identifikasi masalah sebelumnya, maka didapatkan rumusan masalah sebagai berikut:

1. Bagaimana mendeteksi serangan *Malware* pada sistem?
2. Apa solusi yang tepat untuk mengatasi serangan *Malware*?
3. Bagaimana peran SIEM sebagai monitoring terhadap serangan *Malware*?

1.4 Batasan Masalah

Berdasarkan rumusan masalah sebelumnya, maka didapatkan Batasan masalah sebagai berikut:

1. Penelitian hanya difokuskan pada direktori yang menandakan terjadinya serangan *Malware*.
2. Penelitian ini menggunakan sistem operasi Windows 10, Debian 11 dan *tool* VirusTotal dalam pengujiannya.
3. Penelitian ini memanfaatkan aplikasi Wazuh untuk memantau *event real-time* serangan terhadap sistem.
4. Penelitian ini menggunakan *environment virtual*.

1.5 Tujuan Penelitian

Berdasarkan Batasan masalah sebelumnya, tujuan penulis melakukan penelitian ini adalah sebagai berikut:

1. Mengidentifikasi serangan *Malware* pada sistem.
2. Menganalisa kemampuan SIEM dalam mengatasi masalah, khususnya serangan *Malware*.
3. Menjelaskan hasil analisis yang nantinya akan menghasilkan solusi untuk serangan *Malware*.

1.6 Manfaat Penelitian

Adapun manfaat yang didapat melalui penelitian ini adalah sebagai berikut:

1. **Bagi Penulis**
    a. Untuk melengkapi salah satu syarat kelulusan Strata Satu (S1), Informatika Fakultas Ilmu Komputer Universitas Pembangunan Veteran Jakarta.
    b. Mendapatkan pengetahuan dan pemahaman mengenai serangan *Malware* serta cara untuk mendeteksi hal tersebut.
2. **Bagi Universitas**
    a. Sebagai bentuk kontribusi karya ilmiah pada disiplin ilmu Informatika.
    b. Sebagai acuan untuk referensi terhadap penelitian di bidang keamanan siber.
3. **Bagi Masyarakat**
    a. Menambah wawasan mengenai keamanan siber.
    b. Sebagai tambahan referensi terhadap penelitian dengan topik serupa.
    c. Memberikan saran pada Organisasi terkait pengawasan di bidang keamanan siber.

1.7 Sistematika Penulisan

Dalam sistematika penulisan proposal ini, disusun berdasarkan aturan penulisan yang terdiri dari beberapa bagian, yaitu:

BAB 1: PENDAHULUAN

Bab ini menjelaskan latar belakang penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, ruang lingkup, luaran yang diharapkan, dan sistematika penulisan.

BAB 2: TINJAUAN PUSTAKA

Bab ini berisi uraian teori – teori yang mendasari penelitian secara detail, dapat berupa metode, model, algoritma, teknik, konsep, prosedur, atau definisi yang berkaitan dengan topik penelitian.

BAB 3: METODOLOGI PENELITIAN

Bab ini menjelaskan tahapan penelitian, deskripsi pendekatan teoritis, desain eksperimen, delineasi wilayah kajian, sumber data, teknik pengumpulan data, teknik pengolahan data, dan teknik

analisis data, yang digunakan untuk mencapai tujuan penelitian. Untuk setiap proses yang dijalankan, harus dijelaskan dasarnya.

BAB 4: HASIL DAN PEMBAHASAN

Bab ini menjelaskan mengenai penerapan atau implementasi dari metodologi penelitian yang ada di bab sebelumnya.

BAB 5: KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan dari hasil percobaan di Bab 4 dan saran untuk penelitian selanjutnya.

DAFTAR PUSTAKA

RIWAYAT HIDUP

LAMPIRAN