LAPORAN
PRAKTIKUM KEAMANAN INFORMASI 1
UNIT 4
ANALISIS ANATOMI MALWARE

DISUSUN OLEH:

Nama : Yana Dayinta Nesthi
Kelas : RI4AA
NIM : 21/478358/SV/19272
Dosen Pengampu : Anni Karimatul Fauziyyah, S.Kom., M.Eng.

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
2023

ANALISIS ANATOMI MALWARE

A. TUJUAN

- Meneliti dan menganalisis malware

B. DASAR TEORI

1. Malware

Malware merupakan software yang dibuat dengan tujuan untuk memasuki atau merusak sistem komputer, server, atau jaringan komputer tanpa mendapatkan izin atau persetujuan dari pemiliknya. Malware dapat menyebabkan kerusakan pada sistem komputer dan juga dapat menyebabkan pencurian data atau informasi. Biasanya, malware disebabkan oleh unduhan perangkat lunak ilegal yang dapat menyisipkan malware ke dalam sistem. Terdapat berbagai jenis malware, seperti virus, worm, trojan horse, rootkit, spyware, adware yang terinfeksi, serta software lain yang berbahaya dan tidak diinginkan oleh pengguna komputer.

Malware adalah sebuah istilah yang mengacu pada seluruh perangkat lunak yang digunakan untuk melakukan pencurian, manipulasi, penghapusan, atau bahkan pengintipan sistem tanpa persetujuan. Malware merupakan jenis perangkat lunak yang berbahaya.

Penyebaran malware bisa dilakukan melalui berbagai metode, seperti melalui jaringan internet, email, pesan pribadi, atau halaman situs web. Tak hanya perangkat komputer, bahkan server situs web juga rentan menjadi korban dari malware.

C. ALAT DAN BAHAN

- PC
- Akses internet

D. HASIL DAN ANALISIS

Sesuai dengan yang tercantum pada website:https://www.malwarebytes.com/blog/threats
Saya mendapatkan hasil sebagai berikut:

1. Generic.Malware/Suspicious

Malwarebytes mengidentifikasi file-file yang mencurigakan dengan nama Generic.Malware/Suspicious. File-file tersebut menunjukkan ciri-ciri yang mengindikasikan bahwa mereka mungkin merupakan malware, yaitu jenis perangkat lunak yang dimaksudkan untuk menyebabkan kerusakan pada sistem komputer, perangkat, atau jaringan. Malware bersifat bermusuhan, mengganggu, dan sengaja merugikan. Ia berusaha untuk menginvasi, merusak, atau menonaktifkan perangkat dengan mengambil kontrol atas operasinya.

2. Exploit.CVE202121551.Vulnerable

Exploit.CVE202121551.Vulnerable merupakan nama deteksi yang diberikan oleh Malwarebytes untuk sebuah driver Dell bernama dbutil_2_3.sys

yang rentan terhadap serangan eksploitasi. Driver Dell tersebut memiliki kerentanan kontrol akses yang tidak memadai yang dapat menyebabkan peningkatan hak akses, penolakan layanan, atau pengungkapan informasi. File driver ini mungkin telah terpasang di sistem operasi Windows Dell Anda saat menggunakan berbagai paket utilitas pembaruan firmware seperti Dell Command Update, Dell Update, Alienware Update, Dell System Inventory Agent, atau Dell Platform Tags. Hal ini termasuk saat menggunakan solusi pemberitahuan Dell apa pun untuk memperbarui driver, BIOS, atau firmware di sistem Anda.

3. **HackTool.AutoKMS**

HackTool.AutoKMS merupakan istilah deteksi generik yang digunakan oleh Malwarebytes untuk mengidentifikasi hacktool yang dirancang untuk memungkinkan penggunaan ilegal produk Microsoft seperti Windows dan Office. Hacktool merupakan jenis perangkat lunak risiko khusus yang dikenali oleh keamanan komputer. Secara umum, perangkat lunak risiko (riskware) merujuk pada item yang tidak sepenuhnya berbahaya tetapi memiliki potensi risiko bagi pengguna di cara lain. HackTool.AutoKMS kadang-kadang mengandung backdoor dan seringkali ditemukan pada situs web dengan reputasi yang kurang terpercaya.

4. **Malware.AI**

Deteksi Malware.AI.(id-nr) adalah hasil dari modul Artificial Intelligence di Malwarebytes 4 dan produk bisnis Malwarebytes. Deteksi malware generik ini terjadi karena adanya sistem tanda tangan otomatis baru kami yang bernama BytesTotal dan mesin DDS yang menggunakan teknologi Machine Learning dengan pembelajaran otomatis 100% tanpa interaksi manusia untuk mengidentifikasi malware. Teknik-teknik ini termasuk dalam mesin Katana Malwarebytes yang dikembangkan untuk mendeteksi secara massal berbagai jenis malware dan adware secara otomatis. Biasanya, nomor id-nr terdiri dari 9 digit.

Namun, setelah pengecekan yang lebih cermat, item-item yang terdeteksi sebagai Malware.AI dapat dikelompokkan lebih tepat berdasarkan perilakunya. Malwarebytes menggunakan kategori-kategori ancaman yang mendasari, antara lain:

- Adware
- Fraudtool
- Hijack
- Ransomware
- Riskware
- Rogue
- Rootkit
- Spyware
- Trojan

- Virus
- Worm

E. KESIMPULAN

Malware adalah perangkat lunak berbahaya yang dibuat tanpa izin untuk memasuki dan merusak sistem komputer, server, atau jaringan. Jenis malware seperti virus, worm, trojan horse, rootkit, spyware, dan adware dapat menyebabkan kerusakan pada sistem dan pencurian data. Malware dapat menyebar melalui internet, email, atau pesan pribadi, dan bahkan dapat menyerang server situs web.

F. DAFTAR PUSTAKA

LABS, M. (n.d.). *Top 10 Protection Lists of February 2023*. Retrieved Maret 7, 2023, from https://www.malwarebytes.com/blog/threats