LAPORAN TUGAS AKHIR KEAMANAN SIBER

ANALISIS MALWARE

Kelompok 2

Anggota Kelompok :

2320506044 – Oktario Mufti Yudha

2340506061 – Restu Wibisono

2340506063 – Zidhan Arzaq Karim

2340506072 – Devan Putra Hersusanto

Prodi Teknologi Informasi Jurusan Teknik Elektro

Fakultas Teknik Universitas Tidar

2024

I. PENDAHULUAN

A. Tujuan Praktikum

1. Identifikasi Ancaman
2. Memahami Cara Kerja Malware

B. Dasar Teori

Malicious software atau malware merupakan segala perangkat lunak yang membahayakan pengguna, komputer ataupun jaringan. Malware terbagi menjadi beberapa jenis yaitu, trojan horses, worms, rootkits, scareware dan spyware.

Analisis malware menggunakan beberapa aplikasi perangkat lunak untuk mengetahui perubahan registry, aktivitas malware di jaringan, dan metadata malware. Hasil dari penelitian tersebut menyebutkan bahwasanya dengan teknik analisis tersebut diperoleh informasi yang lebih lengkap terkait sampel malware.

Pencegahan terhadap insiden malware dapat dilakukan dengan analisis pada malware untuk mengetahui cara kerja dan karakteristik dari malware tersebut. Analisis malware dapat dilakukan dengan dua metode yaitu analisis statis dan analisis dinamis. Menggabungkan kedua metode analisis ini dapat memberikan informasi dan hasil yang lebih lengkap. Informasi yang diperoleh berupa karakteristik dan indikator identik yang menunjukkan adanya keberadaan malware tersebut dalam sistem atau computer.

Dalam pelaksanaannya, dibuat lingkungan khusus yang digunakan untuk proses analisis. Lingkungan khusus ini dapat berbentuk perangkat fisik ataupun mesin virtual. Beberapa perangkat lunak yang dapat digunakan adalah VMWare, Parallels, Xen, Microsoft Virtual PC, dan Wireshark.

II. LANGKAH DAN HASIL PRAKTIKUM

A. Langkah Praktikum

Berikut adalah jawaban untuk soal berdasarkan analisis dari file "SOAL ANALISIS MALWARE.txt", ditambah langkah-langkah yang dapat dilakukan dengan file ”.pcap”:

1. What are the infected file(s) downloaded and their hashes?

Jawaban:

File 1
Nama: AutoIt3.exe
Hash: 237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d
Lokasi: http://getldrrgoodgame.com:2351/

Keterangan: Salinan aplikasi AutoIt3.

File 2
Nama: ralmzl.au3
Hash: 975d1510380171076b122cd556a1a05bd1eca33b98a9fd003fb3662cb8c83571
Lokasi: http://getldrrgoodgame.com:2351/msiomxgnyqu
Keterangan: File skrip berbahaya yang dijalankan oleh AutoIt3.exe.

File 3 (Archive)
Nama: Test_395-3823.zip
Hash: 9d4636ac5dea137d9db154d004ce3d4176aed7c308a09d73e26da1db31bd4332
Keterangan: Arsip ZIP yang memulai infeksi.

File 4 (Script)
Nama: Test_395-3823.vbs
Hash: 36f4de19faa2c9366288d6cb2b65e65bd6a2897bcf0de6835da0cb12cb5574ae
Keterangan: Skrip VBS yang digunakan untuk mengunduh file lain.

2. What URL/Domain of the infected site?

Jawaban:
Domain: getldrrgoodgame.com
URL:

- http://getldrrgoodgame.com:2351/
- http://getldrrgoodgame.com:2351/msiomxgnyqu

3. What is the IP address of the Windows VM that gets infected?

Jawaban:
IP Address: 10.1.2.5
Keterangan: Alamat IP dari VM Windows (DESKTOP-XWSJRLZ) yang terinfeksi.

4. What is the MAC Address of the Windows VM that gets infected?

Cara Menemukan:
MAC Address tidak diberikan di file .txt, tetapi dapat ditemukan di file .pcap dengan langkah-langkah:
Gunakan filter:

arp && ip.addr == 10.1.2.5
MAC Address akan muncul di kolom Source Address.

5. What is the domain name of the compromised website?

Jawaban:
Domain Name: getldrrgoodgame.com

6. What is the IP address and domain name that delivered the exploit kit and malware?

Jawaban:
IP Address: 81.19.135.139
Domain Name: getldrrgoodgame.com

7. What is the domain name that delivered the exploit kit and malware?

Jawaban:
Domain Name: getldrrgoodgame.com

8. Pada menit dan jam berapa serangan pertama kali masuk?

Cara Menemukan:
Gunakan file .pcap dan cari lalu lintas awal ke IP 81.19.135.139.
Filter:

ip.addr == 81.19.135.139

Perhatikan waktu dari paket pertama yang tercatat. Informasi waktu dapat ditemukan di kolom Time di Wireshark.

9. Cari lokasi tempat darimana website / IP Hacker dan yang terlibat tersebut berasal!

Jawaban:
IP Address: 81.19.135.139
Gunakan layanan geolokasi IP seperti:

- https://ipinfo.io
- https://www.abuseipdb.com/

Kemungkinan besar IP ini berasal dari negara tertentu di Eropa Timur atau wilayah lain di mana server malware sering di-host.

10. Jelaskan dengan bahasamu sendiri bagaimana kemungkinan korban bisa terinfeksi, bagaimana malware bisa masuk sistem, dan tujuan dari malware tersebut!

Jawaban:

Kemungkinan korban terinfeksi:

Korban mendownload file arsip ZIP (Test_395-3823.zip) dari sumber yang tidak terpercaya. Setelah file ZIP diekstrak, korban menjalankan file VBS (Test_395-3823.vbs), yang memulai rantai infeksi.

Bagaimana malware masuk sistem:

File VBS mengunduh salinan AutoIt3.exe dan file skrip berbahaya .au3 dari domain getldrrgoodgame.com. Skrip ini dijalankan menggunakan AutoIt3.exe, yang memungkinkan malware memulai komunikasi dengan server Command & Control (C2).

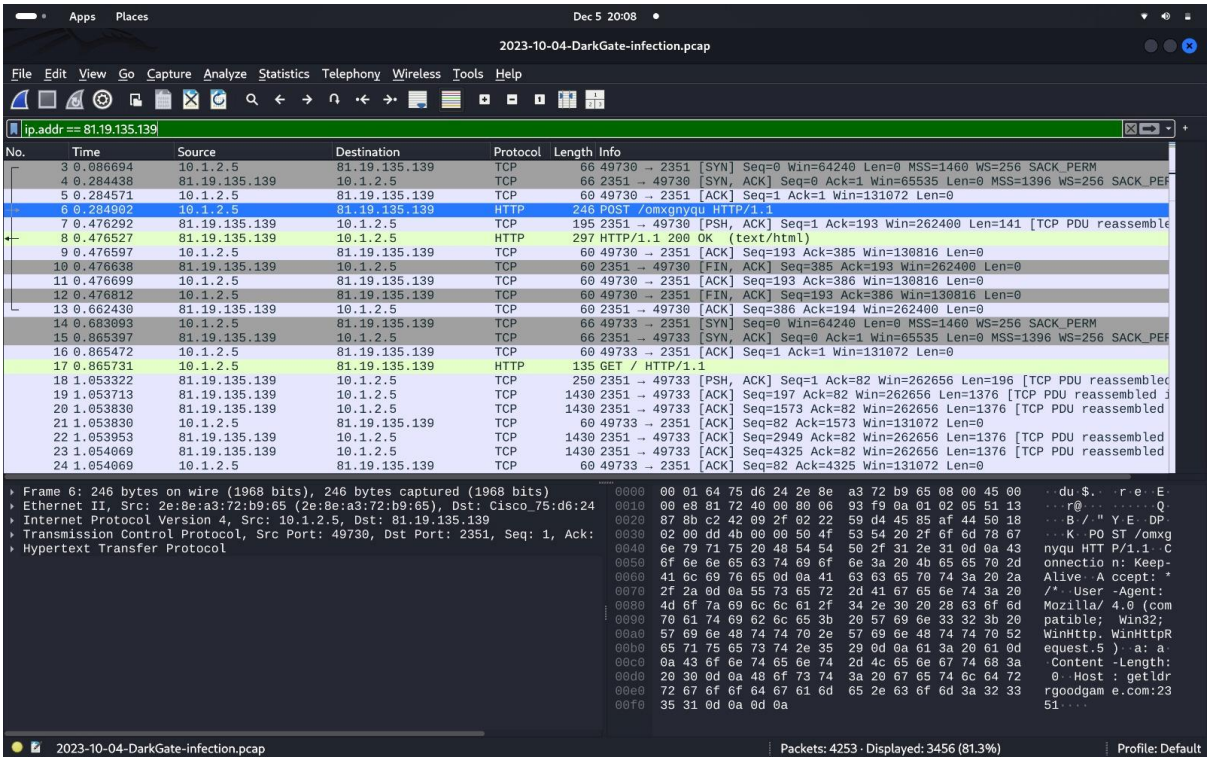
Tujuan malware:

Malware ini digunakan untuk:

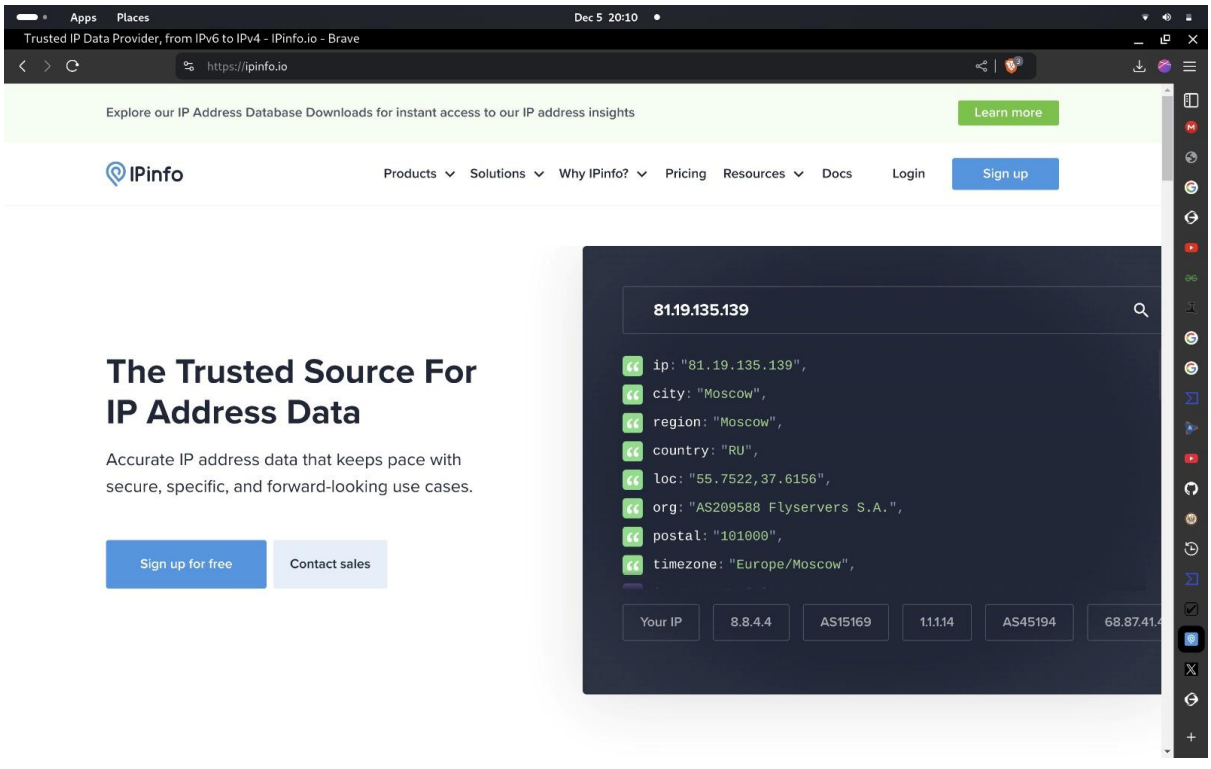
- Menjalankan perintah dari server C2.
- Menginfeksi sistem lebih lanjut dengan modul tambahan.
- Mungkin mencuri data atau menggunakan komputer korban untuk aktivitas berbahaya lainnya seperti botnet.

B. Hasil Praktikum

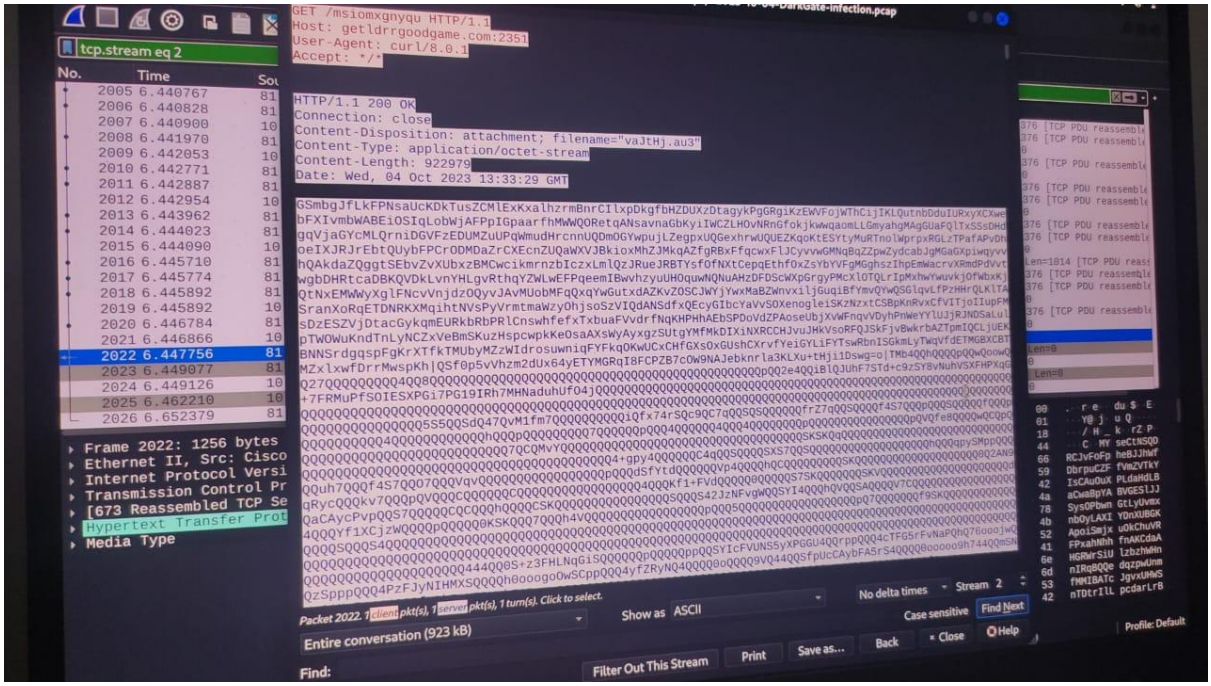
Dokumentasi Gambar-Gambar dalam Analisa Malware



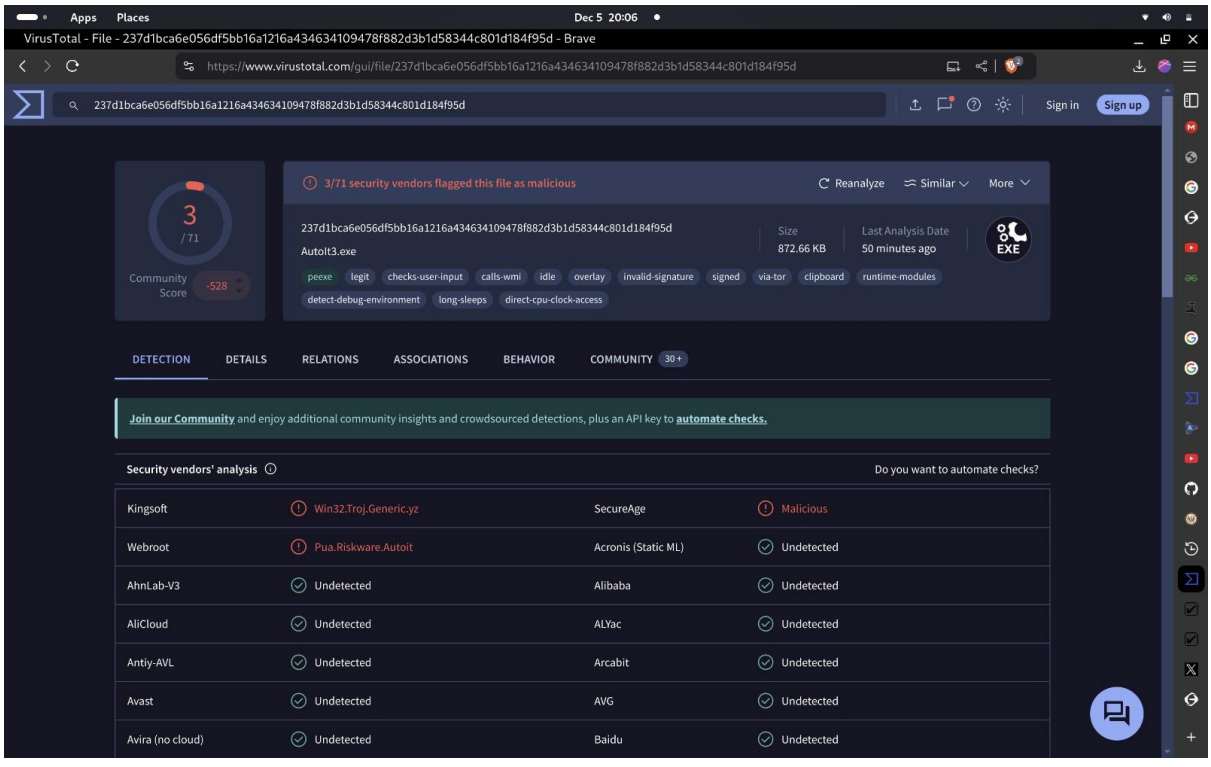
Nb: Gambar No.8



Nb: Gambar No.9



Nb: Gambar Analisis Malware dengan OS Kali Linux



Nb: Gambar dari Virus Total

III. Kesimpulan

Jadi kesimpulannya adalah analisis malware merupakab sebuah proses mengekstraksi informasi dari suatu malware melalui inspeksi statis dan dinamis menggunakan bantuan perangkat lunak, teknik dan proses. Dengan melakukan kegiatan analisis malware, analis akan mengetahui cara kerja suatu malware.