LAPORAN PRAKTIKUM

KEAMANAN INFORMASI 1 (SVRI214404)

Unit 3, Analisis *Malware*

DISUSUN OLEH:

Nama : Reyhan Gusnur Putra

NIM : 21/477927/SV/19223

Hari, Tanggal : Selasa, 28 Februari 2023

Kelas : A

PROGRAM STUDI TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

2023

A. Tujuan

- Meneliti dan menganalisis struktur malware
- Mampu mengembangkan malware trojan dengan Njrat
- Mampu analisis malware dengan metode osint

B. Dasar Teori

Malware adalah perangkat lunak yang dibuat dengan tujuan memasuki dan terkadang merusak sistem komputer, jaringan, atau server tanpa diketahui oleh pemiliknya. Istilah malware diambil dari gabungan potongan dua kata yaitu malicious "berniat jahat" dan software "perangkat lunak". Tujuannya untuk merusak atau mencuri data dari perangkat yang dimasuki. Malware biasanya disusupkan ke dalam jaringan internet. Jika secara manual memasukkan ke dalam komputer korban tentu saja sangat sulit. Jadi kebanyakan peretas melakukan aksinya menggunakan bantuin jaringan internet.

Trojan adalah malware yang memasuki sistem dengan cara menyamar sebagai file lain yang seolah aman, kemudian merusak sistem di dalamnya. Hal ini yang membuat trojan berbahaya karena sulit dikenali. Kamu bisa saja tidak sengaja mengunduh trojan yang dikemas dalam bentuk software atau tautan berbahaya.

Trojan juga dikenal dengan nama Trojan Horse. Istilah ini muncul bukan tanpa alasan, sebetulnya ada peristiwa sejarah dibalik nama ini. Istilah Trojan Horse mengadaptasi dari cerita Yunani kuno, yaitu masa Perang Troya.

OSINT berasal dari dua istilah yakni "Open Source" dan "Intelligence". "Open Source" mengacu pada informasi apapun yang diperoleh dari internet secara online. Sedangkan yang dimaksud "Intelligence" adalah informasi yang sudah dikumpulkan untuk tujuan profesional. Sehingga dapat kita definisikan OSINT sebagai informasi apa pun yang dapat dikumpulkan secara legal dari sumber publik yang terbuka secara bebas tentang individu atau organisasi. Dalam praktiknya, OSINT tidak hanya informasi yang didapatkan dari internet, tetapi bisa juga berupa informasi berupa teks seperti surat kabar, gambar, video, webinar, dan bahkan pidato publik semuanya termasuk dalam istilah tersebut.

C. Alat dan Bahan

1. PC atau laptop
2. Jaringan internet
3. Software Njrat

D. Tugas dan hasil

1. Kerjakan modul praktikum unit 4 no 1 dan 2 analisis struktur malware
    a. Menggunakan mesin pencari favorit Anda, lakukan pencarian untuk malware terbaru. Selama pencarian Anda, pilih empat contoh malware, masing-masing dari jenis malware yang berbeda, dan bersiaplah untuk membahas detail tentang apa yang dilakukan masing-masing, bagaimana masing-masing ditransmisikan, dan dampak masing-masing penyebabnya.
        - Ransomware artinya program tebusan, yaitu sebuah program jahat (malicious software) yang dapat mengunci, menghapus, dan mengambil data tertentu dari perangkat target. Setelah ransomware masuk ke dalam perangkat Anda, program tersebut akan mengunci file, program, atau data digital lainnya. Ini mengakibatkan Anda tidak dapat mengakses atau menggunakan data tersebut. Selanjutnya, pelaku cybercrime tersebut dapat meminta tebusan jika Anda ingin mendapatkan password untuk membuka file tersebut.
        - Virus trojan adalah sebuah malware yang sering menyamar sebagai file, email, bahkan link yang seolah-olah berasal dari lembaga resmi. Trojan adalah malware yang dapat membuat para peretas memiliki akses bebas ke dalam device Anda. Mereka bisa mencuri dan mengacaukan sistem yang ada pada perangkat tersebut.
        - Exploit kit adalah seperangkat program yang digunakan penyerang untuk melakukan serangan terhadap kerentanan yang telah diketahui dalam perangkat lunak/software. Cara kerja exploit kit adalah dengan memanfaatkan kerentanan kemanan korban ketika korban sedang menjelajahi internet.
        - PUP adalah singkatan dari Potentially Unwanted Program, dalam artian adalah program yang terunduh meskipun tidak diinginkan oleh pengguna tersebut, contohnya seperti Adware ataupun Spyware. Biasanya PUP ini akan menumpang/disisipkan pada aplikasi/software gratis yang diinstal oleh pengguna, aplikasi/software ini biasa disebut Freeware. Bagaimanapun juga PUP tidak bisa dikatakan ilegal, karena pengguna sendiri yang memberikan izin akses untuk aplikasi/software tersebut. Meskipun dikatakan demikian, keberadaan PUP sangatlah mengganggu penggunanya. Umumnya PUP

menampilkan iklan pop up dan pada setiap website yang dikunjungi akan selalu muncul iklan.

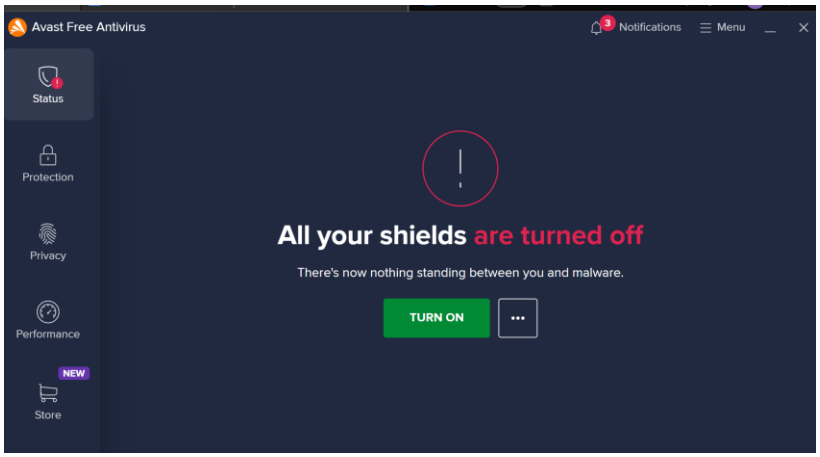
b. Baca informasi tentang malware yang ditemukan dari pencarian Anda di langkah sebelumnya, pilih salah satu dan tulis ringkasan singkat yang menjelaskan apa yang dilakukan malware, cara penularannya, dan dampaknya.

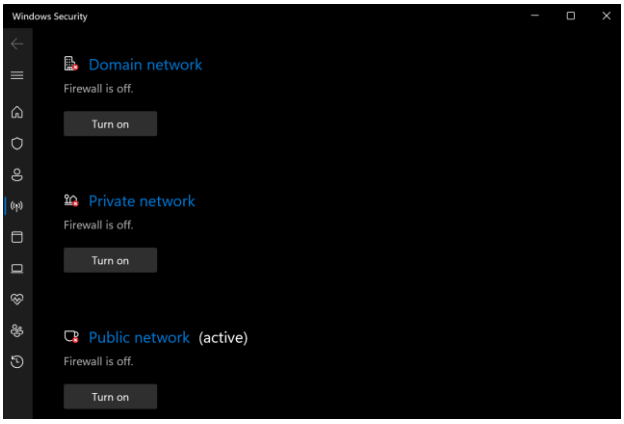
- Malware merupakan perangkat lunak yang bekerja dengan memasuki komputer tanpa perizinan serta dapat menyebabkan kerusakan pada sistem, server, dan jaringan komputer. Malware merupakan gabungan dari kata malicious yang berarti jahat atau berbahaya dan software yang berarti perangkat lunak. Lebih buruk, malware dapat melakukan pencurian data dan informasi yang tersimpan dalam komputer serta menjadi pintu belakang masuknya hacker.Malware dapat masuk pada sistem komputer dengan melalui jaringan internet. Umumnya, perangkat lunak ini disisipkan pada unduhan pada situs web ilegal, iklan, email phishing, dan lain lain. Malware tidak diciptakan oleh sembarang orang. Perangkat lunak ini diciptakan oleh para hacker yang memiliki pemahaman tinggi akan perangkat lunak dengan tujuan tertentu. Melalui berbagai cara dan serta jenisnya yang beragam, malware mampu menimbulkan masalah pada perangkat. Berikut merupakan dampak dari serangan malware pada perangkat:
    1. Memperlambat sistem komputer
    2. Kerusakan data dan dokumen
    3. Kendala pada aplikasi di dalamnya
    4. Sistem tidak dapat dibuka
    5. Perubahan data menjadi virus

2. Develop malware trojan dengan Njrat.

   Berikut adalah langkah untuk mengembangkan malware trojan dengan Njrat.

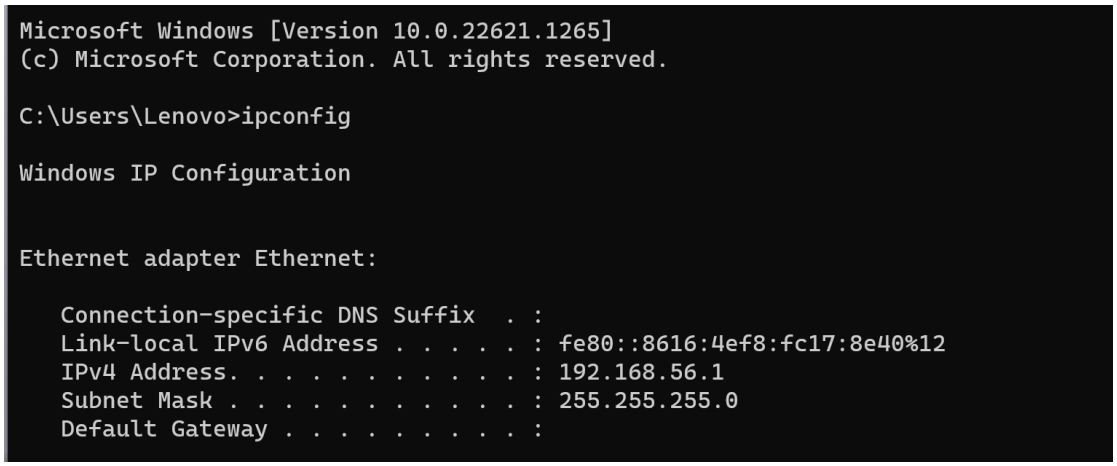
   1. Langkah pertama matikan semua software antivirus dan *Firewall* pada kedua komputer yang akan digunakan untuk percobaan njRAT.

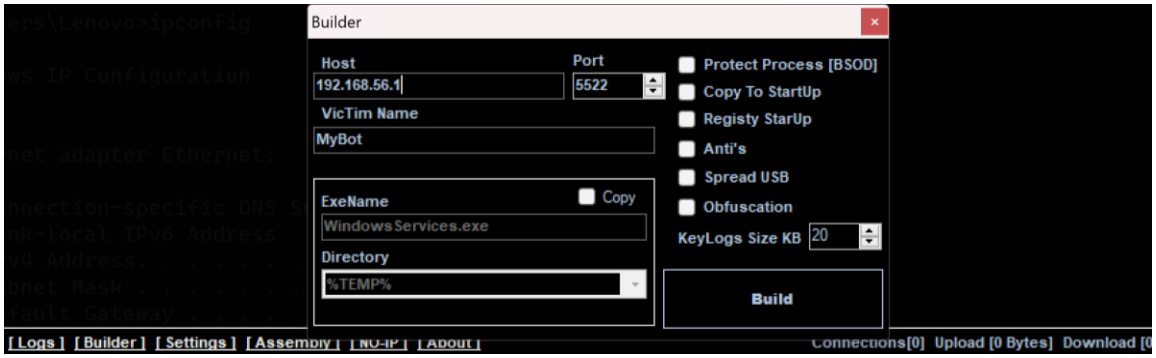




2. Install dan ekstrak software njRAT, kemudian jalankan aplikasi njRAT pada komputer host.
3. Jika sudah menjalankan *software* njRAT, maka akan muncul menu awal untuk memasukkan nomer port. Masukkan port 5522.

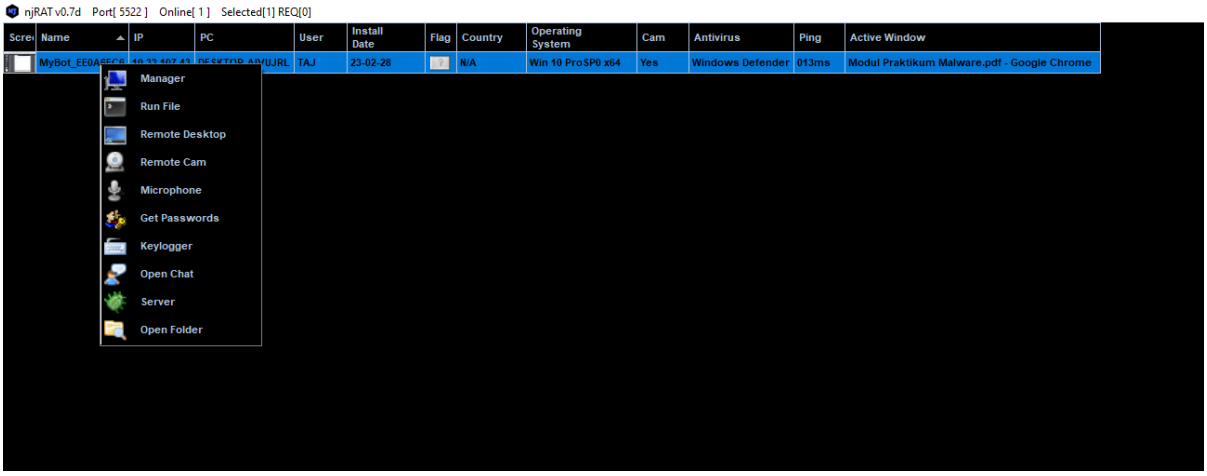
4. Selanjutnya klik fungsi ”Builder” untuk membuat trojan untuk dimasukkan ke PC atau laptop *victim*. Masukkan IP PC atau laptop host, untuk mencari tahu IP device yang digunakan, buka command prompt lalu ketik “ipconfig” lalu klik enter. Jika sudah memasukkan IP address, klik build.



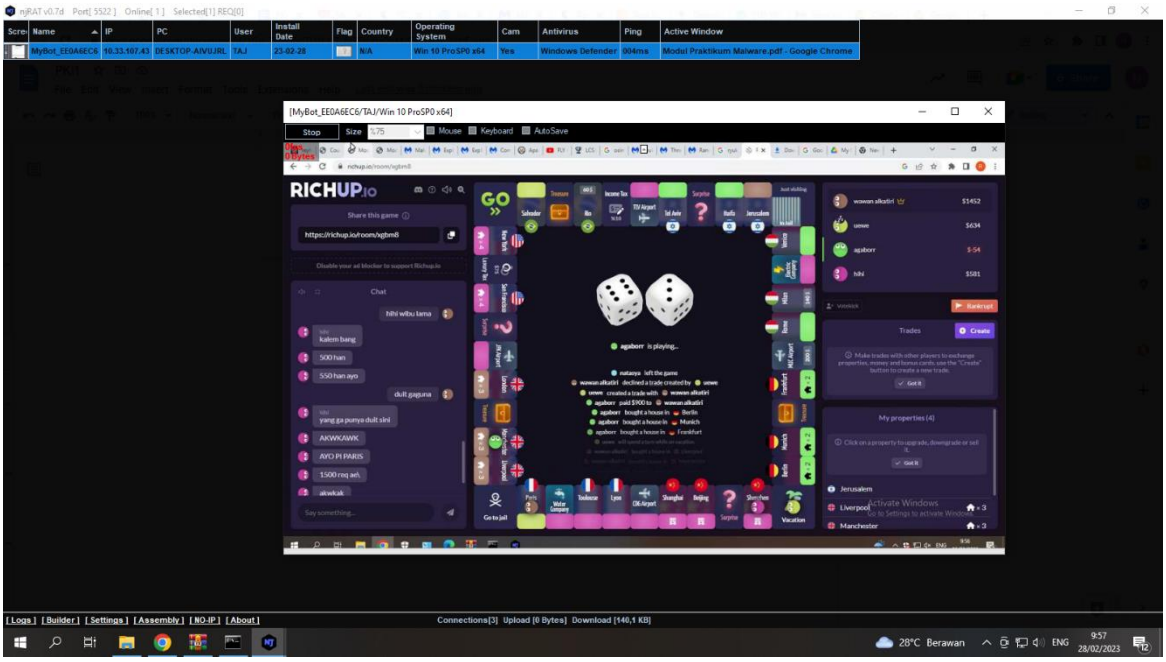


5. Simpan file tersebut pada tempat yang diinginkan device host.

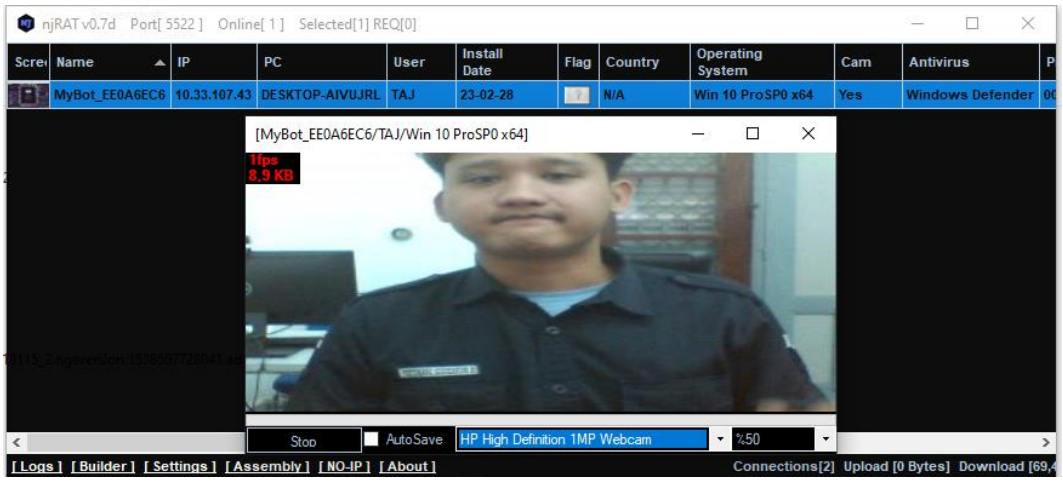
6. Kemudian *copy* hasil file yang sudah dibuat kedalam komputer victim, lalu jalankan pada komputer victim. Akan muncul informasi device victim pada device host. Klik kanan pada victim untuk melihat fungsi yang bisa digunakan.



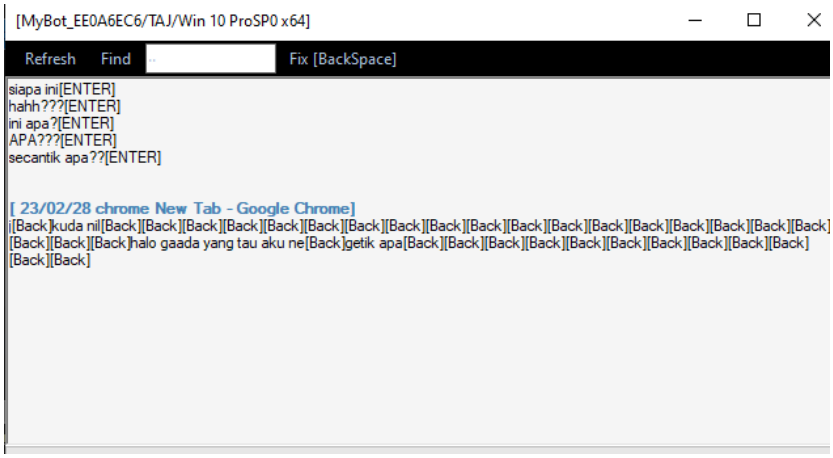
7. Berikut adalah beberapa fungsi njRAT.
    a. Remote desktop



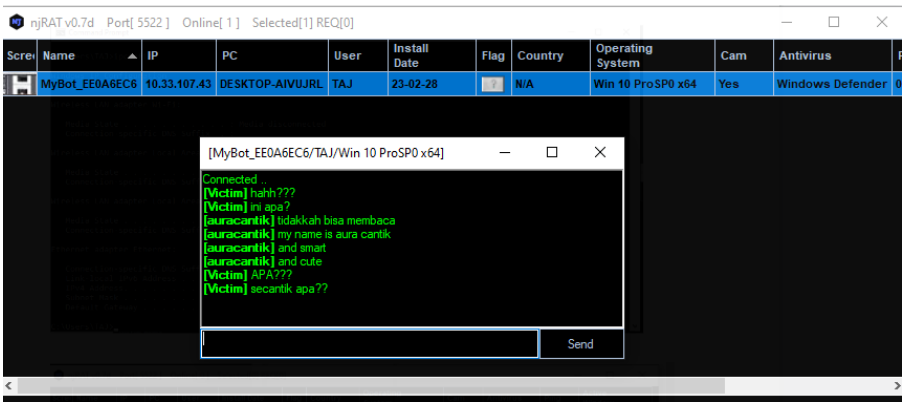
b. Remote cam



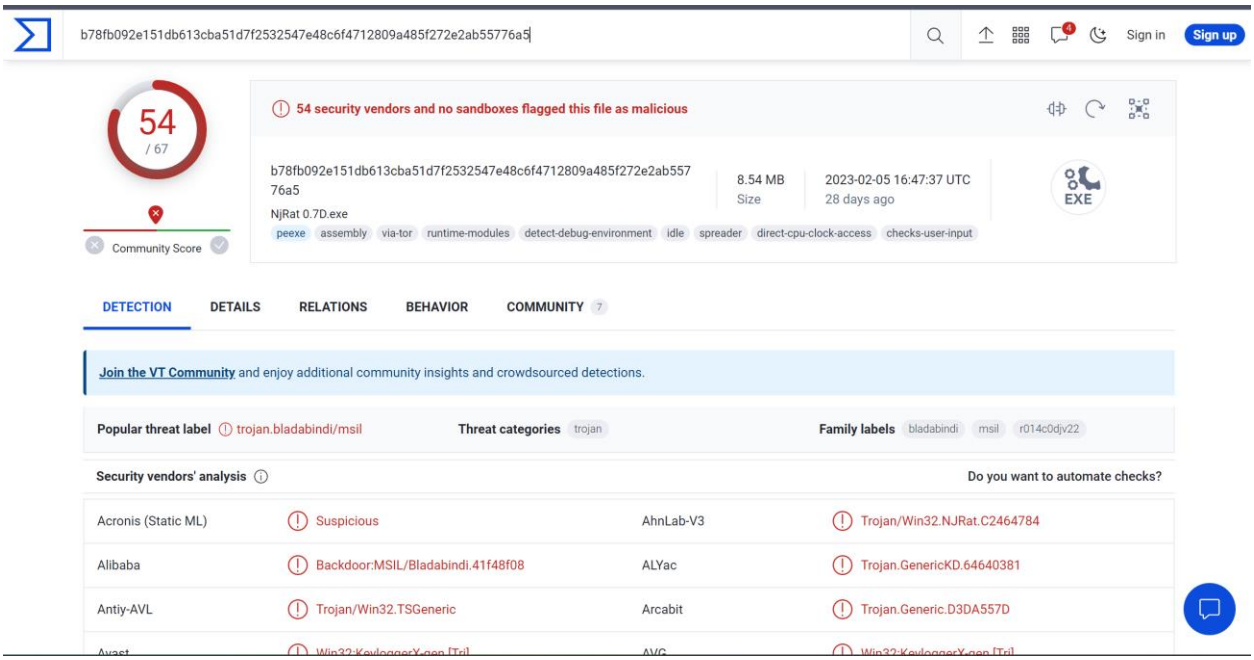
c. Keylogger



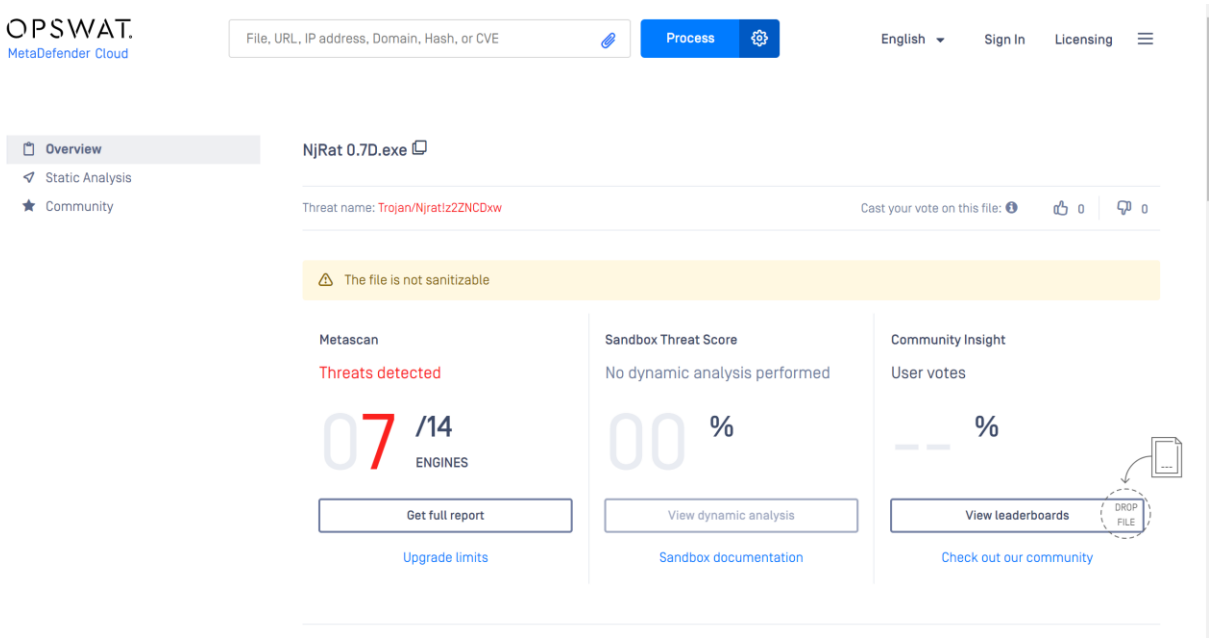
d. Open chat



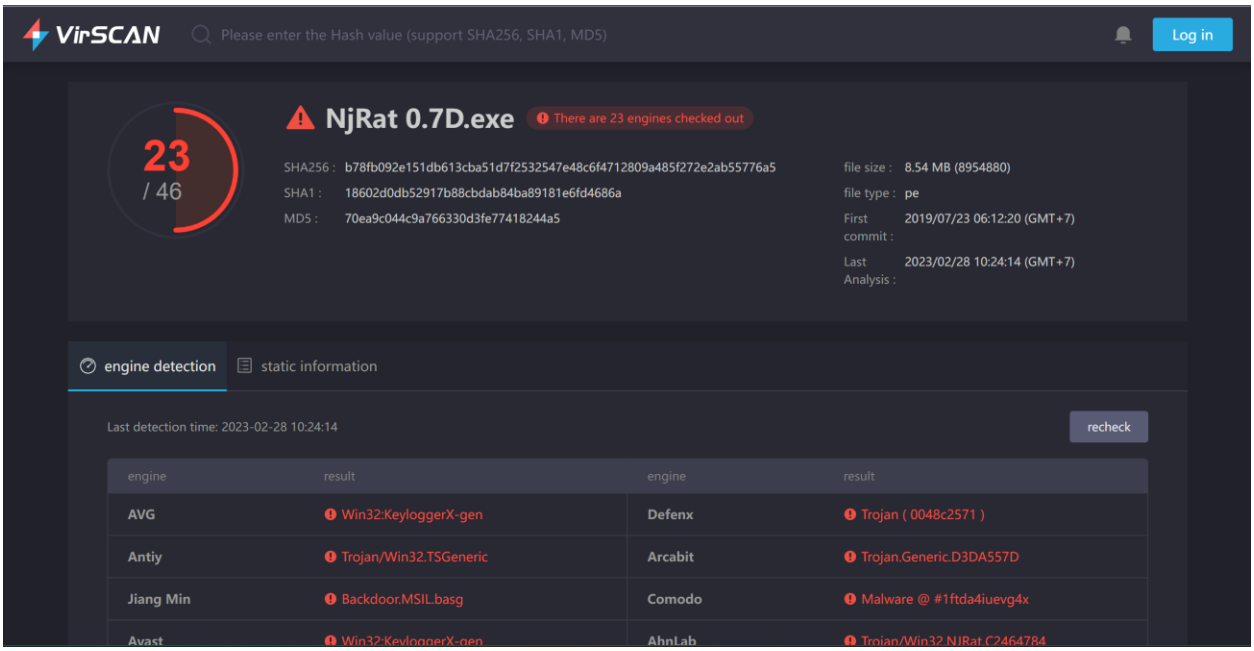
3. Analisis malware dengan metode osint:
    - Virustotal



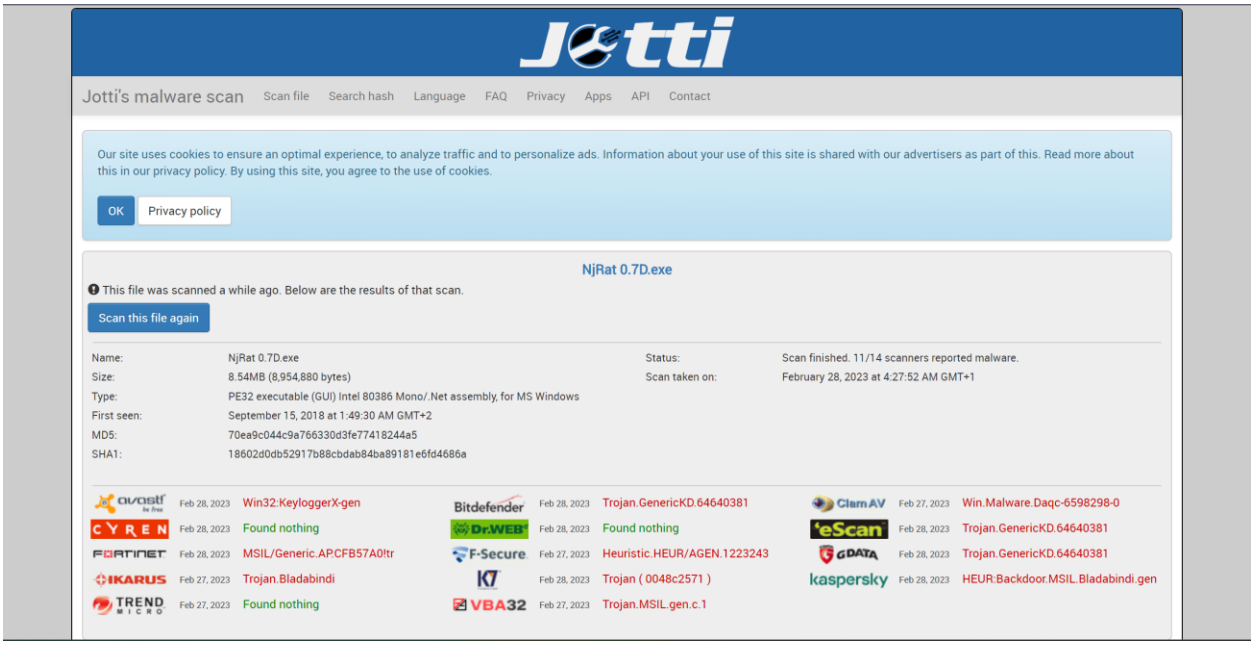
- OPSWAT (Meta Defender)



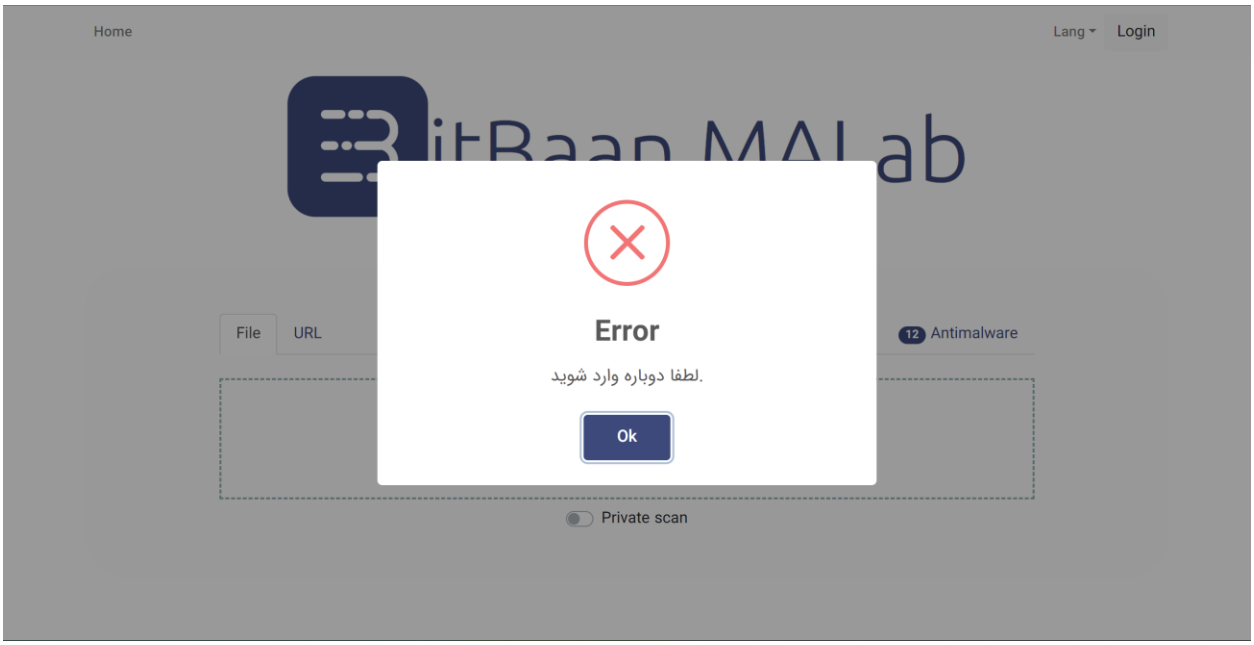
- VirSCAN



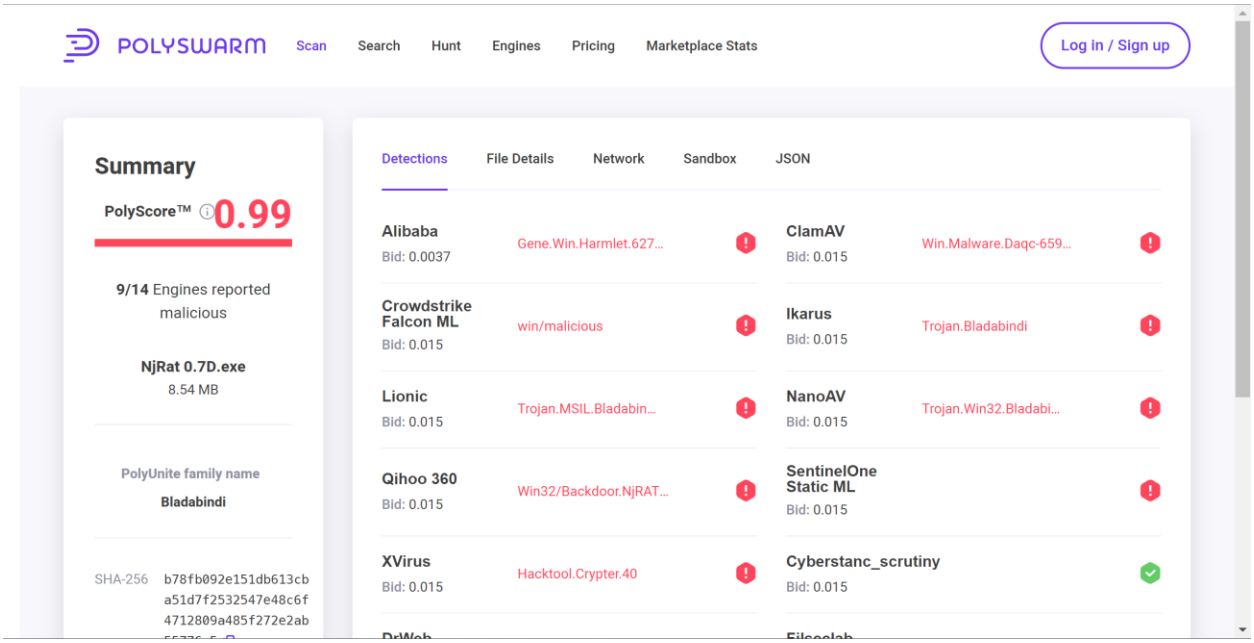
- Jotti



- Bitbaan MaLab



- PolySwarm



E. Analisis

Praktikum kali ini membahas tentang malware, malware atau *Malicious Software* yang berarti program berbahaya yang dibuat secara khusus untuk menyusup sehingga bisa

tetap berada di dalam sebuah sistem untuk periode waktu tertentu tanpa sepengetahuan pemilik sistem tersebut. Biasanya, malware menyamarkan diri menjadi program yang bersih. Berbagai macam software berbahaya yang dapat ditemukan, terlebih di era dunia digital seperti saat ini. Dengan jenis dan kategori ancaman baru muncul, pengguna harus semakin waspada terhadap jenis malware yang beredar. Sebuah penelitian menemukan bahwa jenis malware yang paling umum sekarang adalah Trojans dan worms. Pada praktikum kali ini kita mencoba menggunakan virus trojan bernama njRAT. Trojan adalah sebuah program jahat yang menyamar menjadi sebuah program yang berguna bagi komputer. Jika korban menginstal trojan pada komputer mereka maka peretas dapat mengakses komputer korban dari jarak jauh. Pada praktikum ini kita mencoba beberapa fitur njRAT, kita bisa mengakses camera dan mikrofon PC/laptop korban, sehingga pelaku dapat memantau korban dari kamera dan mikrofon mereka. Selain mengakses kamera dan mikrofon, pelaku dapat mengambil alih cursor dan keyboard korban. Fitur lain yang dimiliki adalah keylogger yang berfungsi untuk merekam aktivitas pada keyboard komputer korban sehingga pelaku dapat mengetahui apa saja yang diketik oleh korban. Pelaku juga dapat mengakses file-file dan system komputer korban.

Sebagian besar software anti-virus dapat mendeteksi njRAT sebagai trojan sehingga user dapat mengetahui bahwa software yang mereka unduh mengandung file trojan atau tidak. Namun dalam percobaan praktikum, tidak semua software dan web pendeteksi virus dapat mendeteksi file-file berbahaya. Menurut website VirusTotal, hanya 54 dari 67 security vendor dapat mendeteksi bahwa software njRAT berbahaya, dari 14 engine OPSWAT (MetaDefender) hanya 7 yang dapat mendeteksi bahwa njRAT berbahaya. Menurut website VirSCAN, hanya 23 dari 46 engine mereka mampu mendeteksi bahwa njRAT berbahaya. Selanjutnya, website Jotti mengatakan bahwa 3 dari 14 software anti-virus tidak dapat mendeteksi file tersebut berbahaya, kemudian 9 dari 14 engine website PolySwarm mendeteksi bahwa njRAT berbahaya. Tetapi pada website BitBaan MALab tidak bisa melakukan scanning pada software njRAT.

F. Kesimpulan

Kesimpulan yang didapat dari praktikum ini adalah:

1. Sebuah virus tidak dapat 100% terdeteksi oleh software maupun website pendeteksi anti-virus. Namun pengguna dapat mengamankan perangkat dari deteksi dari software maupun website pendeteksi anti-virus
2. 1 antivirus software dapat mendeteksi sebagian besar virus yang ada di internet.
3. Malware adalah perangkat lunak yang dibuat dengan tujuan memasuki dan terkadang merusak sistem komputer, jaringan, atau server tanpa diketahui oleh pemiliknya.

G. Daftar Pustaka

Dewaweb Team. 2022. *Apa itu Malware? Pengertian, Jenis dan Cara Mengatasinya.* Diakses pada 6 Maret 2023. https://www.dewaweb.com/blog/pengertian-malware-pentingnya-dewaguard/

Shinra, Amelia. 2023. *Ketahui Apa itu Trojan, Jenisnya dan Cara Menghindarinya.* Diakses pada 6 Maret 2023. https://www.dewaweb.com/blog/apa-itu-trojan/#:~:text=Trojan%20adalah%20malware%20yang%20memasuki%20sistem%20dengan%20cara,berbahaya.%20Trojan%20juga%20dikenal%20dengan%20nama%20Trojan%20Horse.