# LAPORAN PRAKTIKUM
# KEAMANAN INFORMASI 1
# UNIT 4


**DI SUSUN OLEH:**

| | |
|---|---|
| Nama | : Bintang Nur K |
| NIM | : 21/481453/SV/19790 |
| Kelas | : RI4AA |
| Hari, tanggal | : Selasa, 28 Februari 2023 |
| Dosen Pengampu | : Anni Karimatul Fauziyyah, S.Kom., M.Eng |
| Asisten Praktikum | : Gabriella Alvera Chaterine |

**PROGRAM SARJANA TERAPAN (DIV)**
**TEKNOLOGI REKAYASA INTERNET**
**DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA**
**SEKOLAH VOKASI**
**UNIVERSITAS GADJAH MADA**
**2023**

# UNIT 4
# ANALISIS ANATOMY MALWARE

## I. TUJUAN

- Meneliti dan menganalisis malware

## II. LATAR BELAKANG

*Malware* merupakan perangkat lunak yang dapat merusak sistem, jaringan, dan server 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

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.

NjRAT adalah salah satu tools hacking untuk *OS windows* yang digunakan untuk meremote pc satu dengan pc lain. RAT adalah singkatan dari *Remote Administrator Tool* yang di gunakan untuk menghubungkan dan mengatur satu atau lebih komputer dengan berbagai kemampuan seperti:

- Screen/camera capture atau control
- File management (download/upload/execute/dll.)
- Shell control (CMD control)
- Computer control (power off/on/log off)
- Registry management (query/add/delete/modify)
- Password management

## III. ALAT DAN BAHAN

Alat dan Bahan yang dibutuhkan untuk melaksanakan praktikum adalah

- PC Host
- Koneksi Internet
- File Njrat

## IV. LANGKAH KERJA DAN HASIL

**1)** 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.

Contoh jenis malware antara lain: Ransomware, Trojan, Hoax, Adware, Malware, PUP, Exploit, Exploit Kit dan Kerentanan. Cari malware dengan mengunjungi situs web berikut menggunakan istilah pencarian berikut:

- Dasbor Lanskap Ancaman Pusat Ancaman McAfee
- Pusat Ancaman Malwarebytes Labs (10 Malware Teratas)
- Securityweek.com > ancaman virus > virus-malware
- Technewsworld.com > keamanan > malware

Jawab:

a. Ransomware adalah salah satu jenis *malware* yang bekerja dengan metode enkripsi mengolah data menjadi kode yang tidak dapat dibaca oleh perangkat.

b. PUP (Potentially Unwanted Program) adalah program yang terunduh meskipun tidak diinginkan oleh pengguna tersebut, contohnya seperti *Adware* ataupun *Spyware*

c. Trojan

adalah malware yang memasuki sistem dengan cara menyamar sebagai file lain yang seolah aman, kemudian merusak sistem di dalamnya.

d. Worm

Worm tidak menginfeksi data atau program, tapi dia akan menyalin dirinya untuk menyusupi komputer lainnya melalui jaringan yang bisa memberi beban pada sistem operasi komputer dan bandwith jaringan.

**2)** 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.

Jawab:

Ransomware adalah salah satu jenis *malware* yang bekerja dengan metode enkripsi mengolah data menjadi kode yang tidak dapat dibaca oleh perangkat. Sehingga, menyebabkan korban tidak dapat mengakses perangkatnya sebelum data tersebut didekripsi diolah kembali dari bentuk yang sudah dienkripsi agar dapat dibaca oleh perangkat.

Ransomware secara umum ada 2 jenis

- *Locker ransomware*, yaitu *ransomware* yang mengunci akses pengguna ke sistem atau perangkat
- *Crypto ransomware*, yaitu *ransomware y*ang menghalangi penggunauntuk mengakses *file* atau data, baik dengan enkripsi *file* atau metode lain.

Cara serangan ransomware:

*Ransomware* menyerang dengan menggunakan *trojan* yang disamarkan menjadi *file* atau aplikasi tidak berbahaya, kemudian penggunakan melakukan suatu aksi pada *trojan* tersebut, baik berupa *download* (unduh) atau membukanya

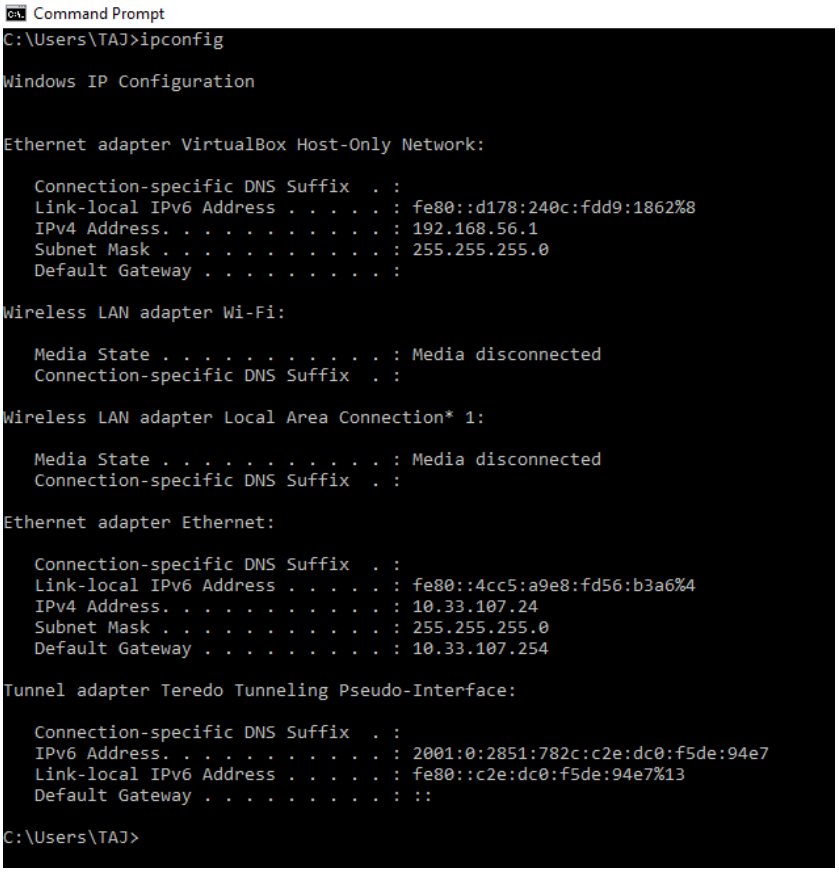
Ransomware dapat mengacaukan sistem perangkat hingga tidak dapat dioperasikan.Selain itu, Ransomware juga memiliki sifat yang dapat menyebar dan menginfeksi perangkat di sekitarnya. Sehingga, sangat berbahaya jika tidak segera ditangani dengan cepat.

**Pada praktikum Malware NJRAT**

1. Jalankan virtual machine windows
2. Clone VM windows, untuk di jadikan target
3. Pada VM Windows yang dijadikan host matikan semua antivirus dan firewall pada kedua komputer yang digunakan untuk memakai aplikasi njrat ini.
4. Download dan ekstrak aplikasi NJRAT kemudian run aplikasi NJRAT pada komputer host. https://github.com/adarift/njRAT/releases/tag/v0.7D

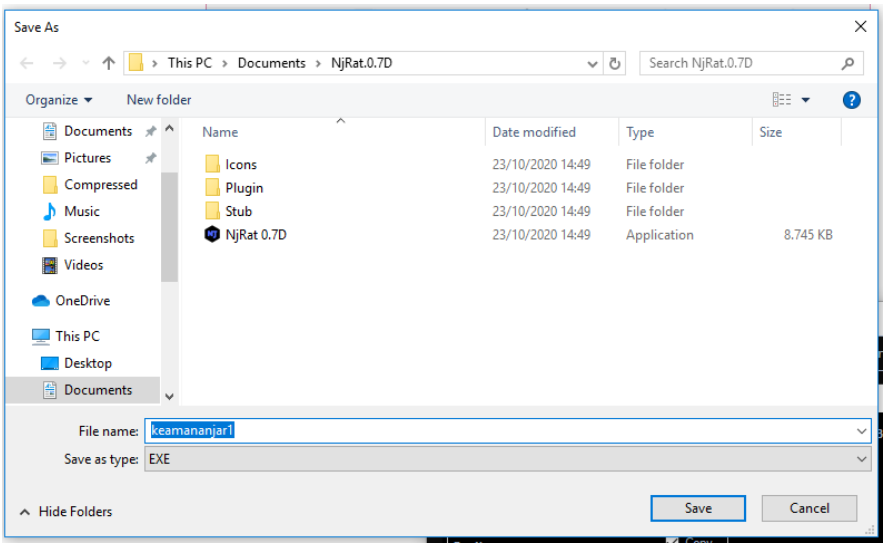
   Masukkan port yang ingin digunakan 5522

5. Sebelumnya, cek IP Address milik host terlebih dahulu. IP ini nantinya akan digunakan oleh NJRAT, dan pastikan juga komputer victim berada pada satu jaringan.

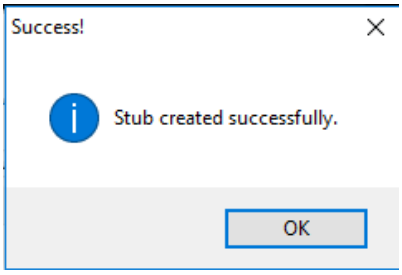



6. Buat aplikasi yang akan dipasang pada komputer victim. Masukkan IP Address host pada kolom host dan port yang sesuai dengan yang kita tentukan tadi pada awal membuka aplikasi NJRAT agar dapat diakses oleh komputer nanti, kemudian klik tombol build.

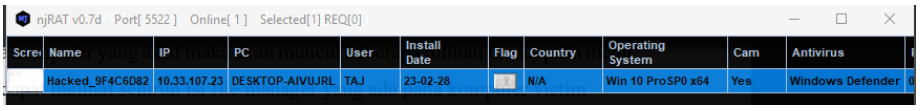
7. Simpan aplikasi hasil build.



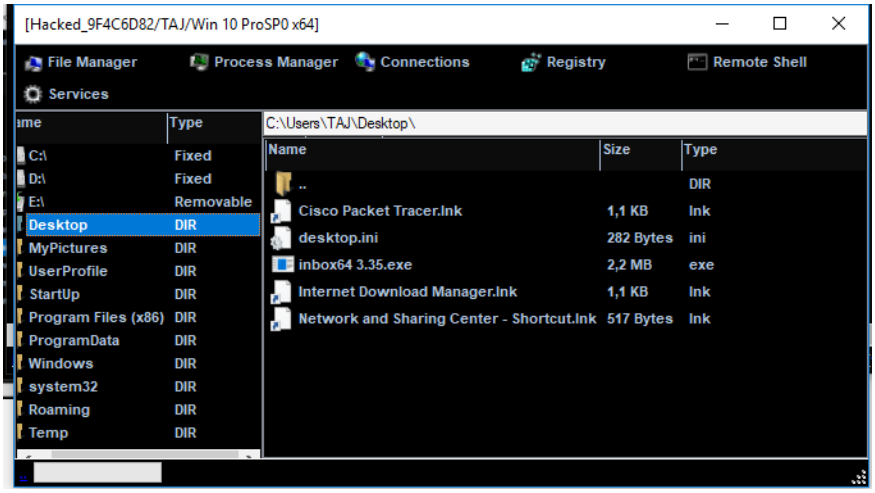

Setelah klik save, maka akan ada notifikasi “stub created successfully”.



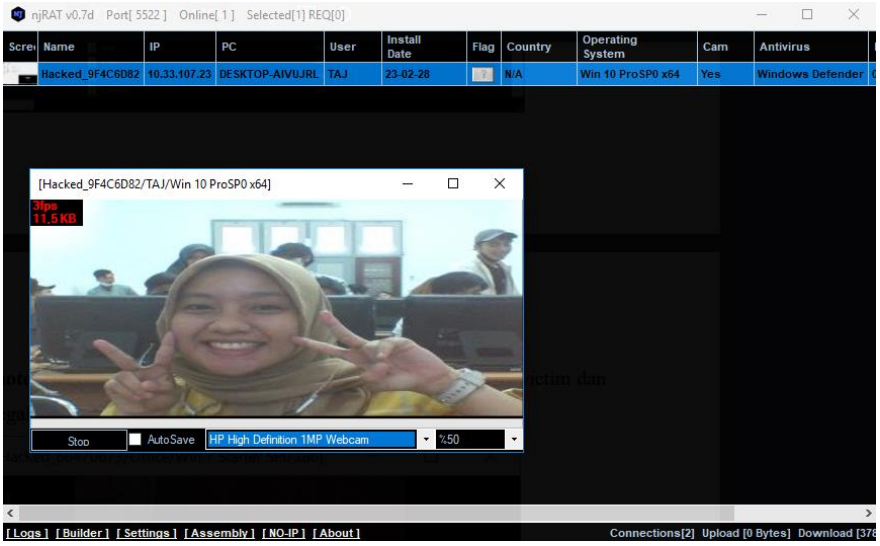

8. Kemudian, copykan aplikasi keamananjaringan.exe yang sudah telah kita buat ke dalam komputer victim. Kemudian, pada komputer victim jalankan aplikasi tersebut. Ketika sudah terpasang pada komputr victim, NJRAT pada host akan mendeteksi komputer victim



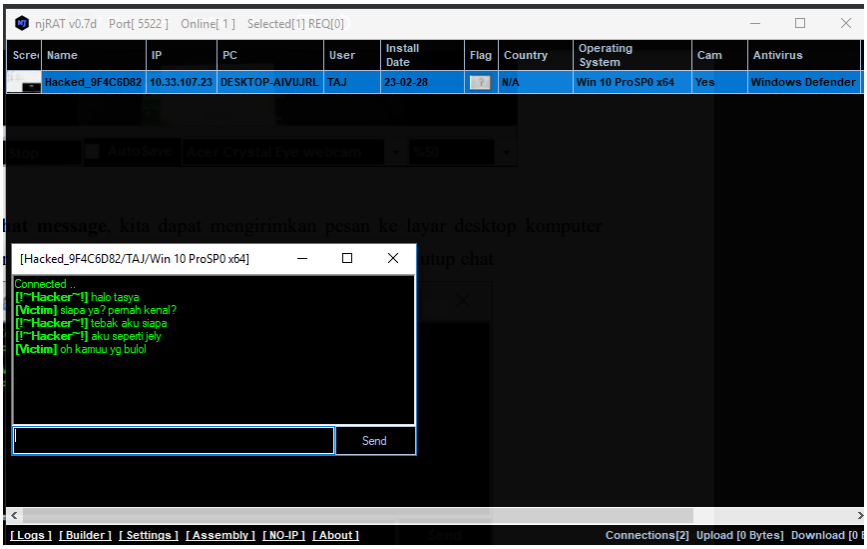
9. Klik kanan pada komputer yang aktif maka akan muncul beberapa pilihan menu, pilih menu manager agar dapat melihat seluruh isi file manager yang ada pada komputer victim



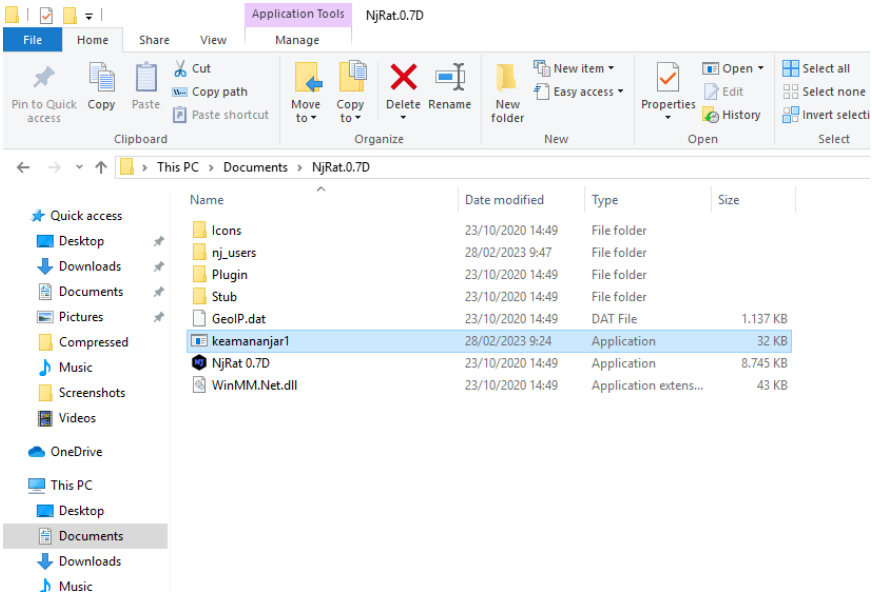

10. Pada menu remote cam maka akan membuka webcam yang ada di komputer victim dan dapat melihat segala aktivitas yang dilakukan oleh victim



11. Pada pilihan chat message, kita dapat mengirimkan pesan ke layar desktop komputer victim, dan user komputer dapat melakukan balasan tanpa bisa menutup chat.




12. Buatlah file trojan dengan nama mahasiswa masing-masing atau nama file Test.exe simpan pada Desktop di VM target

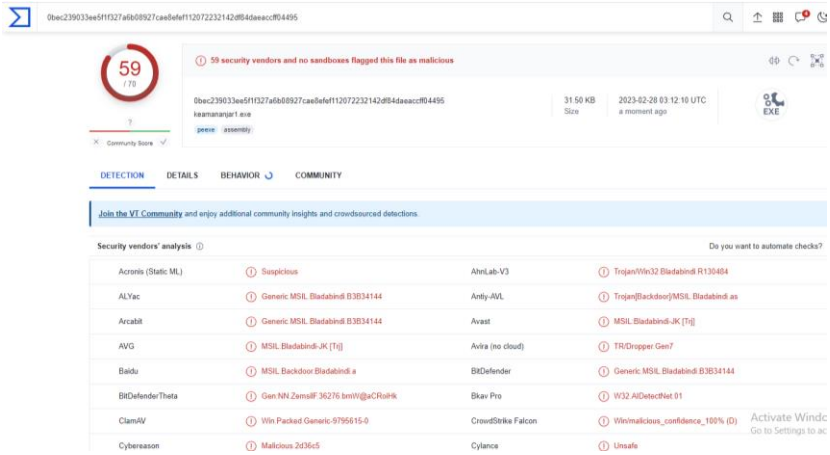


**ANALISIS MALWARE DENGAN METODE OSINT:**

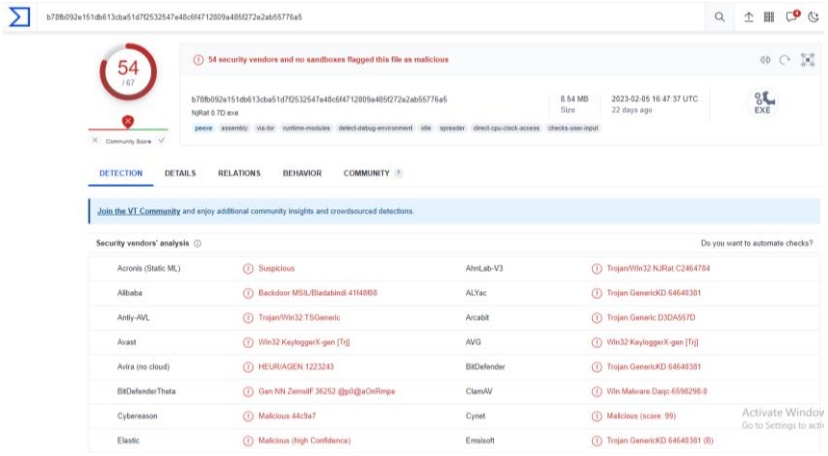
OSINT umumnya merupakan metode pengumpulan data yang lebih murah dibandingkan dengan metode investigasi tradisional. Banyak tools OSINT berbasis langganan, dan menawarkan berbagai paket kepada perusahaan berdasarkan kebutuhan mereka.

## A. VirusTotal

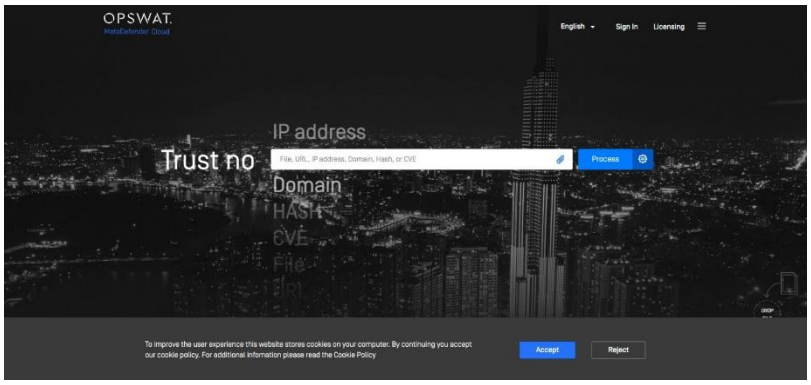
### File NjRAT

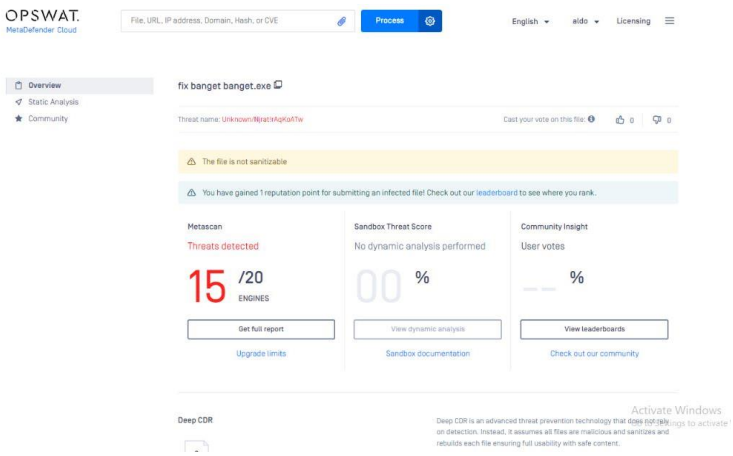



### APK NjRAT



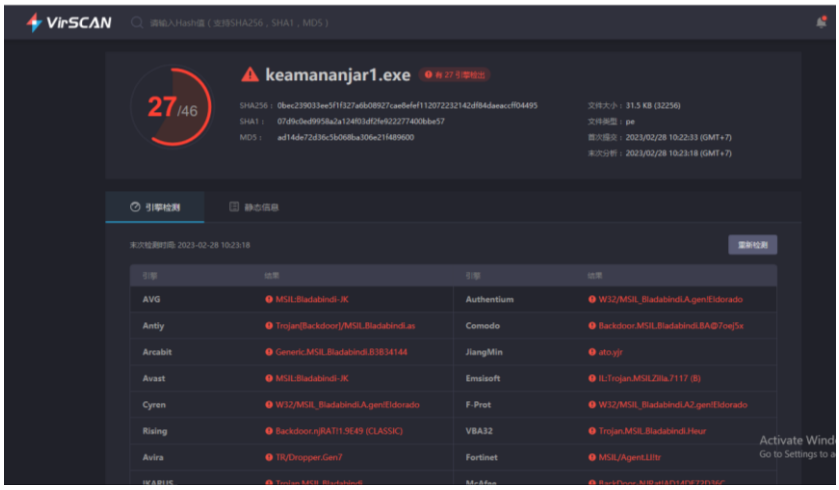
## B. OPSWAT (Meta Defender)



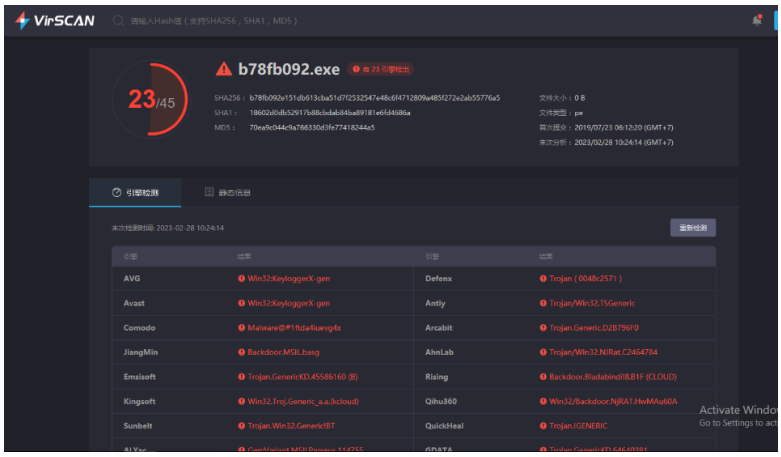




## C. VirSCAN

### File NjRAT

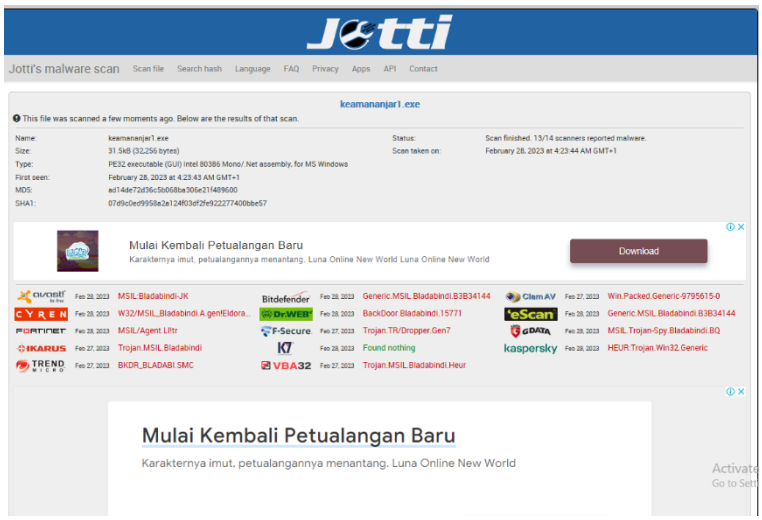


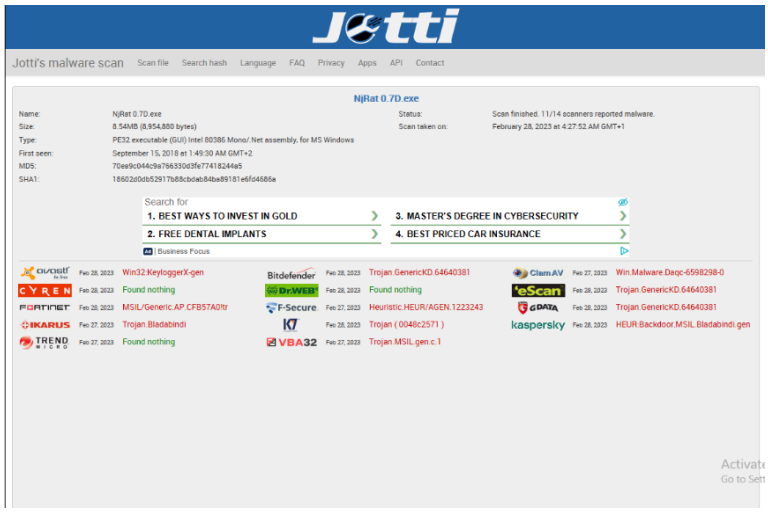
**APLIKASI NjRAT**




## D. Jotti

**File NjRAT**

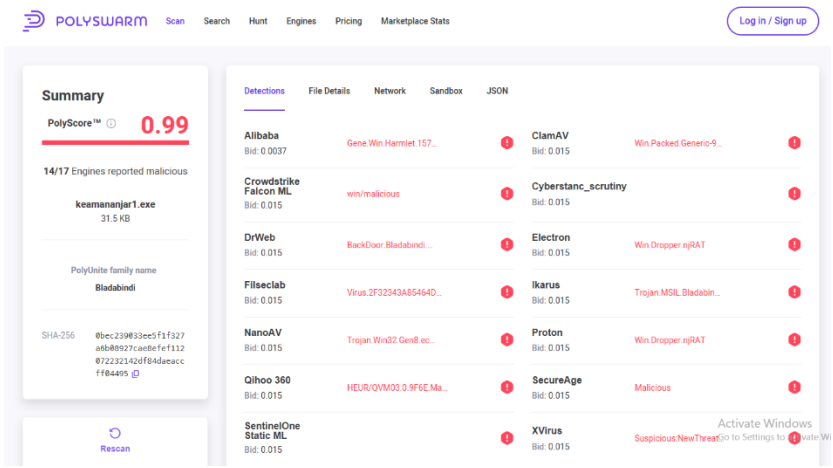


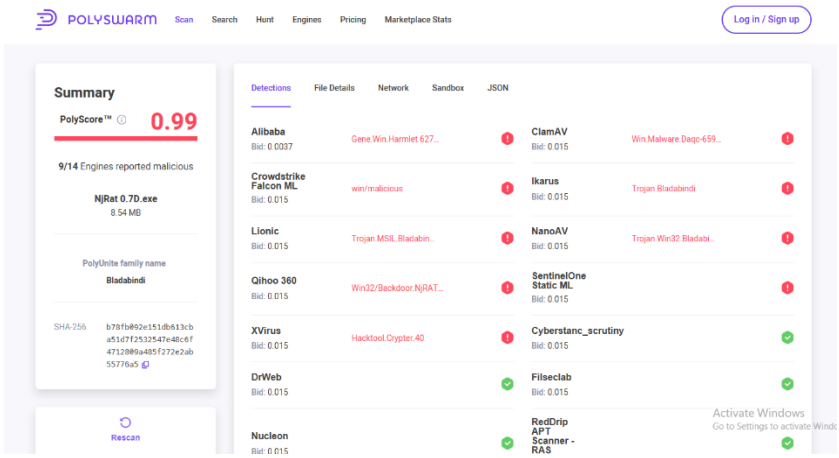
## E. Bitbaan MaLab


## F. PolySwarm

### File NjRAT




### Aplikasi NjRAT



## V. ANALISIS

Pada praktikum kali ini melakukan uji coba hacking pengguna sistem operasi *windows* menggunakan aplikasi NjRAT.

*Trojan* adalah salah satu jenis *malware* yang ikut berkembang di dalamnya, yang memungkinkan *attacker* masuk ke dalam sistem tanpa diketahui oleh pemilik. Aplikasi ini adalah teknik yang menggunakan kelemahan manusia, sehingga *user* tanpa curiga langsung mengeksekusi sebuah program yang tidak dikenal. Aktivitas *malware* berkaitan erat dengan performa PC dan juga aktifitas *network* pada *system computer.*

Pada langkah awal yang dilakukan adalah pastikan bahwa antivirus dan firewall dari kedua PC yang terhubung baik itu host maupun victim dalam keadaan non-aktif. karena aplikasi ini akan dideteksi sebagai malware.

Lalu untuk dampak perubahan yang terjadi pada PC Target terlihat pada performa masing-masing PC yang telah disisipkan *malware.*

Buka aplikasi NJRAT, masukkan port yang digunakan sesuai dengan keinginan yaitu 5522. Cek ip address host dengan buka CMD (Command Prompt) masukkan perintah ‘ipconfig;, ip ini yang nanti akan diakses oleh NJRAT. Pastikan juga bahwa IP Address milik victim pc berada pada 1 jaringan.

Untuk membuat aplikasi yang didalamnya terdapat Trojan yang nantinya akan dipasangkan pada komputer victim, pilih menu Build. masukkan ip address host yang telah kita cek sebelumnya pada kolom host dan port sesuai dengan port yang kita masukkan sebelumnya agar dapat diakses oleh komputer host nanti, kemudian simpan file yang telah dibuat dan berikan ke komputer korban. Ketika komputer korban menjalankan file tersebut, maka komputer korban telah terjangkit Trojan dan dapat diakses melalui komputer host. Klik kanan pada list komputer yang telah menjadi korban. maka akan ada beberapa pilihan untuk memonitoring dan mengakses komputer korban. Pada pilihan file manager, kita bisa melihat isi seluruh directori dari drive komputer korban, kita dapat melakukan unduh dan unggah file secara bebas.

Pada pilihan remote cam, kita bisa menjalankan kamera pada komputer korban, Pada pilihan remote desktop, kita dapat mengontrol kegiatan mouse dan keyboard pada komputer korban. Pada pilihan chat message, kita dapat mengirimkan pesan ke layar desktop komputer korban, dan user komputer korban dapat melakukan balasan tanpa bisa menutup chat, Ketika aplikasi selesai digunakan, kita dapat menutup koneksi dengan menggunakan menu ‘close’.

Teknik yang digunakan untuk mengumpulkan dan memproses *Open Source Information.*

Pertama**,** strategi dan framework harus jelas untuk memperoleh dan menggunakan *Open Source Intelligence*.

Tidak disarankan untuk menggunakan pendekatan OSINT dengan perspektif sendiri walaupun kita dapat menemukan sesuatu informasi yang menarik atau bermanfaat. Dengan banyaknya informasi yang tersedia melalui sumber terbuka hanya akan membuat kita kewalahan jika tidak menggunakan *framework* yang jelas. Sebagai gantinya, kita harus tau persis apa tujuan kita menggunakan OSINT, misalnya untuk mengidentifikasi atau memulihkan kelemahan pada jaringan kita, dan kemudian memfokuskan pencarian secara khusus untuk tujuan tersebut.

Kedua**,** kita harus mengidentifikasi perangkat atau tools dan teknik yang digunakan untuk mengumpulkan dan memproses *Open Source Information*.

Tanpa adanya perencanaan yang jelas, dan dengan jumlah informasi yang tersedia terlalu besar maka prosesnya menjadi tidak efektif.

## VI. KESIMPULAN

Setelah melaksanakan praktikum yang saya dapatkan adalah

- Malware (malicious software) adalah sebuah sebutan untuk sistem perangkat lunak yang diciptakan untuk merusak suatu sistem pada computer, *Malware NjRAT* termasuk jenis *Trojan horse*
- Trojan dirancang untuk merusak, mengganggu, mencuri, atau secara umum menimbulkan beberapa tindakan berbahaya pada data atau jaringan.
- Trojan menyebabkan komputer menjadi lambat, merusak sistem operasi perangkat, dan bahkan mampu mencuri data penting milik korban.

## VII. DAFTAR PUSTAKA


Alfiyahweb. (2017, January 29). *Hack Komputer Dengan Aplikasi njrat*. Teknik Informatika. Retrieved March 6, 2023, from https://alfiyahweb.wordpress.com/2017/01/29/hack-komputer-dengan-aplikasi-njrat/

Bersama, I. (2020, February 24). *Malware – njrat (remote access trojan)*. -. Retrieved March 6, 2023, from https://ilmubersama.com/2020/02/24/malware-njrat-remote-access-trojan/

Shinta, A. (2023, February 27). *Ketahui Apa Itu trojan, Jenisnya Dan Cara Menghindarinya*. Blog Dewaweb. Retrieved March 6, 2023, from https://www.dewaweb.com/blog/apa-itu-trojan/#:~:text=Lalu%20sebenarnya%2C%20apa%20efek%20dari,mencuri%20data%20penting%20milik%20korban.