# LAPORAN

## Praktikum Keamanan Informasi 1

## Pertemuan Ketiga


Disusun Oleh :

| | | |
|---|---|---|
| Nama | : | Akbar Mertza Satya Putra |
| NIM | : | 21/482067/SV/19895 |
| Kelas | : | RI4AA |
| Dosen Pengampu | : | Anni Karimatul Fauziyyah, S.Kom., M.Eng. |
| Hari, Tanggal | : | Selasa, 28 Februari 2023 |

SARJANA SAINS TERAPAN TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

2023

# Unit 4

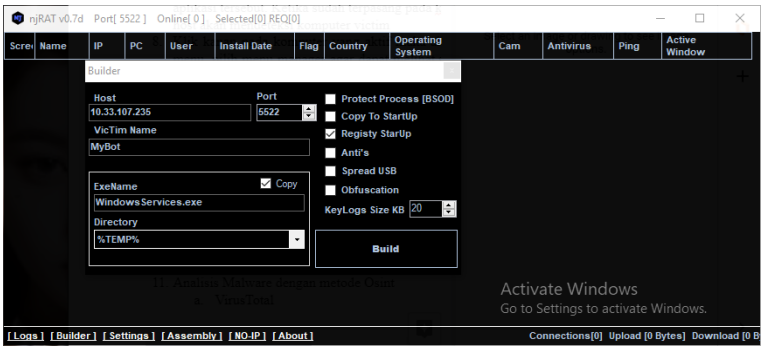
## Analisis Anatomy Malware

A. Tujuan
    1. Meneliti dan menganalisis malware
B. Landasan Teori

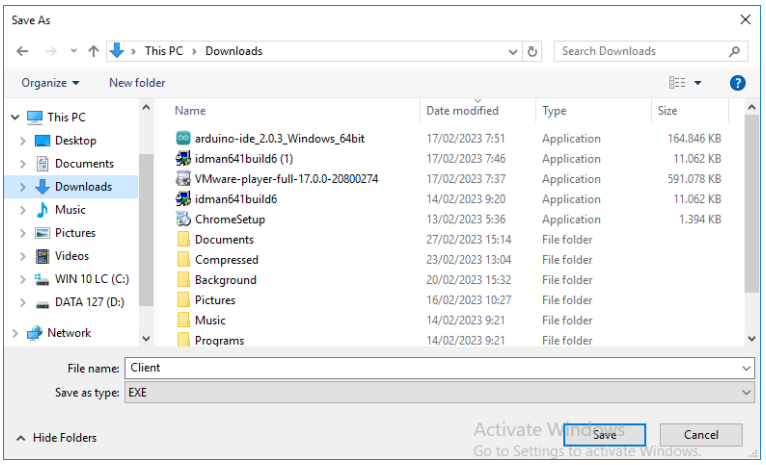
    Malware, atau perangkat lunak berbahaya, mengacu pada berbagai program perangkat lunak berbahaya yang dapat digunakan untuk menyebabkan kerusakan pada sistem komputer, mencuri data, dan melewati tindakan keamanan. Malware juga dapat menyerang infrastruktur penting, menonaktifkan layanan darurat, menyebabkan jalur perakitan membuat produk yang cacat, menonaktifkan generator listrik, dan mengganggu layanan transportasi. Pakar keamanan memperkirakan bahwa lebih dari satu juta ancaman malware baru dirilis setiap hari. McAfee Labs Threats Report 2019 menunjukkan penemuan teknik ransomware baru, pengungkapan miliaran akun melalui dump data profil tinggi, eksploitasi web HTTP yang signifikan, kerusakan pada Windows, Microsoft Office, dan Apple iOS, dan serangan lanjutan pada perangkat pribadi IoT. Temukan versi terbaru dari laporan dengan melakukan pencarian web untuk McAfee Labs Threats Report.
C. Alat dan Bahan
    1. PC dengan akses internet
D. Tugas dan Penyelesaian
    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:
        a. Dasbor Lanskap Ancaman Pusat Ancaman McAfee
        b. Pusat Ancaman Malwarebytes Labs (10 Malware Teratas)
        c. Securityweek.com > ancaman virus > virus-malware
        d. Technewsworld.com > keamanan > malware

        https://www.malwarebytes.com/blog/threats
    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.
    3. 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 5520

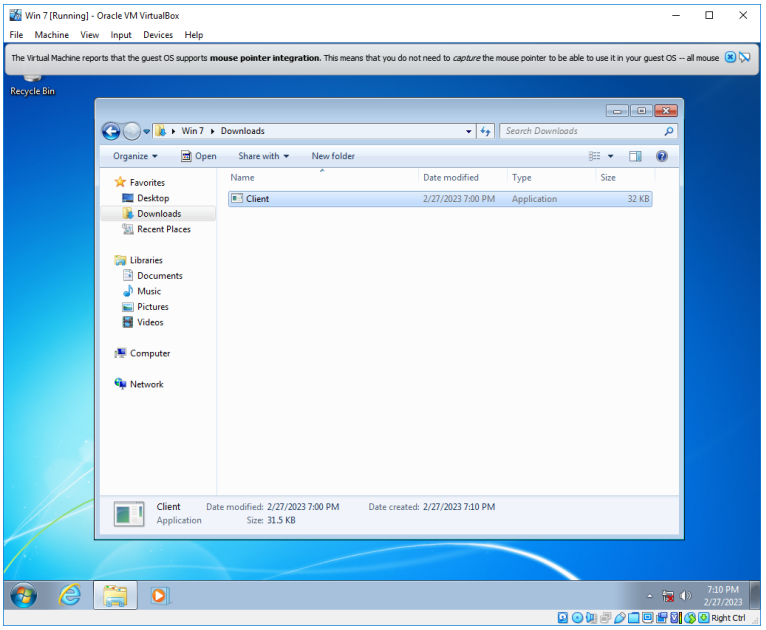

4. Sebelumnya, cek IP Address milik host terlebih dahulu. IP ini nantinya akan digunakan oleh NJRAT, dan pastikan juga komputer victim berada pada satu jaringan
5. Buat aplikasi yang akan dipasang pada komputer victim. Masukkan IP Address host pada kolom host dan port yang sesuai dengan yang kita tentukan tadi pada awal membuka aplikasi NJRAT agar dapat diakses oleh komputer nanti, kemudian klik tombol build




6. Simpan aplikasi hasil build.

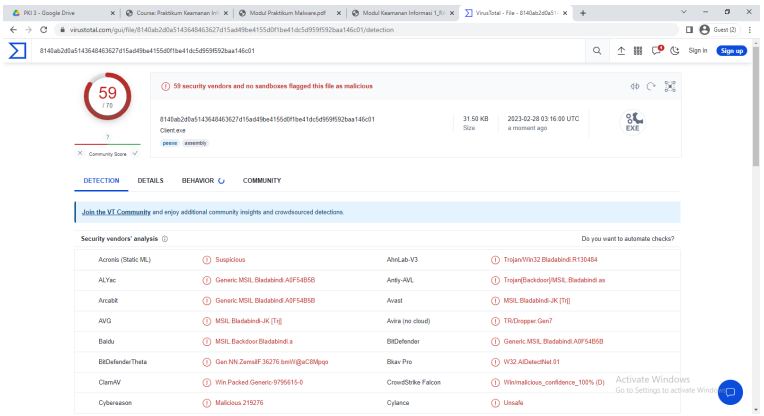



7.
8. Kemudian, copykan aplikasi keamananjaringan.exe yang sudah telah kita buat ke dalam komputer victim. Kemudian, pada komputer victim jalankan aplikasi tersebut. Ketika sudah terpasang pada komputr victim, NJRAT pada host akan mendeteksi komputer victim




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

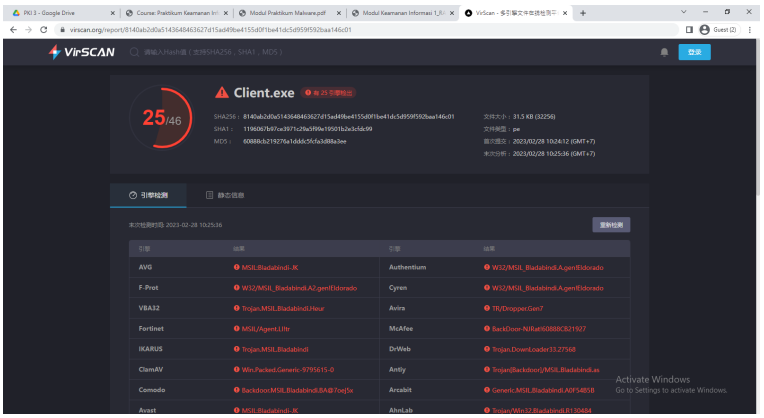
    NJRAT merupakan salah satu malware sejenis Trojan yang menginfeksi komputer victim melalui installasi program. ketika malware terpasang pada PC, maka segala bentuk kegiatan PC victim dapat dimonitoring / dikendalikan melalui PC host yang berada pada satu jaringan melalui akses IP dan port yang telah ditentukan diawal.
12. Analisis Malware dengan metode Osint
    a. VirusTotal




https://www.virustotal.com/gui/file/8140ab2d0a5143648463627d15ad49be4155d0f1be41dc5d959f592baa146c01/detection

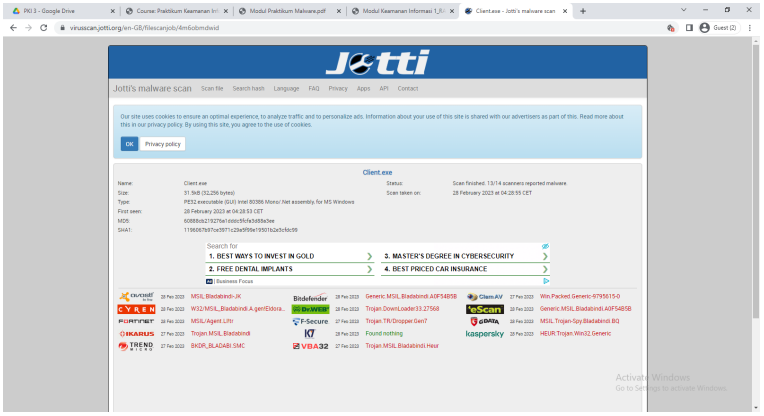
    b. OPSWAT (Meta Defender)

c. VirSCAN




https://www.virscan.org/report/8140ab2d0a5143648463627d15ad49be4155d0f1be41dc5d959f592baa146c01

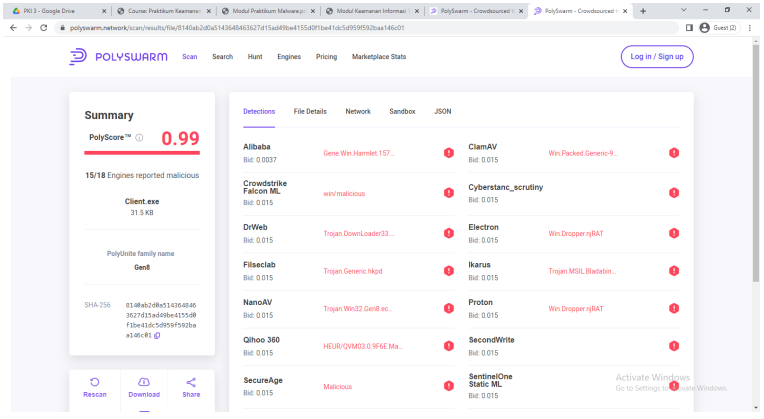
d. Jotti




https://virusscan.jotti.org/en-GB/filescanjob/4m6obmdwid

e. Bitbaan MaLab

f. PolySwarm



E. Pembahasan

Malware adalah perangkat lunak yang dibuat untuk menyusup atau merusak sistem komputer, server atau jaringan komputer tanpa seizin pemiliknya. Malware dapat menyebabkan kerusakan pada sistem komputer dan juga memungkinkan terjadinya pencurian data/informasi.

Analisis statis merupakan proses awal dalam menentukan file yang dicurigai malware sehingga analisis menentukan bahwa file yang dicurigai adalah file yang memiliki kode berbahaya atau disebut malware.

Beberapa malware bekerja dengan menyamar sebagai aplikasi yang tidak berbahaya sehingga meyakinkan pengguna untuk mengunduh dan menggunakan aplikasi tersebut. Ketika aplikasi sudah diunduh dan mulai digunakan, aplikasi akan menyebar dengan cepat dan melihat semua aktivitas komputer.

F. Kesimpulan

Malware adalah perangkat lunak yang dibuat untuk menyusup atau merusak sistem komputer, server atau jaringan komputer tanpa seizin pemiliknya. Malware dapat menyebabkan kerusakan pada sistem komputer dan juga memungkinkan terjadinya pencurian data/informasi.

G. Daftar Pustaka

(n.d.). ANALISIS MALWARE DENGAN TEKNIK STATIC ANALYSIS. Retrieved March 9, 2023, from http://jurnal.lpkia.ac.id/index.php/jkb/article/download/119/106/

*Apa Itu Malware: Pengertian, Jenis, serta Cara Mengatasinya*. (2022, July 15). Cloudmatika. Retrieved March 9, 2023, from https://www.cloudmatika.co.id/blog-detail/apa-itu-malware

*Malware*. (n.d.). EduCSIRT Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi. Retrieved March 9, 2023, from https://educsirt.kemdikbud.go.id/portal/berita/69