# LAPORAN PRAKTIKUM

# KEAMANAN INFORMASI 1

# ANALISIS ANATOMY MALWARE DAN NJRAT


**DISUSUN OLEH**

| | |
|---|---|
| Nama | : Fariansyah Permata Surya |
| NIM | : 21/473155/SV/18810 |
| Hari, Tanggal | : Senin, 06/03/2023 |
| Kelas | : RI4AA |

**SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET**

**DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA**

**SEKOLAH VOKASI**

**UNIVERSITAS GADJAH MADA**

**YOGYAKARTA**

**2022**

## A. Dasar 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.

Remote Access Trojan ini adalah sebuah trojan yang kita buat dan infeksikan ke korban, yang mana setelah trojan berjalan, kita punya hak akses dan kontrol penuh terhadap komputer infeksi tersebut. Tools yang digunakan yaitu njRAT. Aplikasi njRAT ini dulu sangat berjaya ketika Windows XP masih tenar, namun sayang, sekarang ketenarannya sudah mulai berkurang karena sudah banyak antivirus yang dapat mengenalinya. Bahkan si trojan untuk melakukan RAT nya ketika diupload ke virustotal.com, hanya 4 antivirus yang tidak menganggapnya sebagai sebuah trojan. Dibuat menggunakan bahasa pemrograman berbasis .NET sehingga bagi pengguna Windows XP, ada kemungkinan trojan ini tidak dapat dijalankan karena dibutuhkannya .NET framework. Biasanya pengguna njRAT akan menjual akun korban yang terinfeksi trojan hingga menjual generator trojan dan tutorial penggunaannya. Oke, gambar dibawah ini tampilan ketika njRAT pertama kali diaktifkan. Jangan lupa untuk mendisable antivirus dan firewall.

## B. Alat dan Bahan

1. PC Host dengan minimal RAM 8 GB dan Hardisk 40 GB
2. Koneksi Internet

## C. Tugas dan Penyelesaian

### Unit 4

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 masingmasing, bagaimana masing-masing ditransmisikan, dan dampak masing-masing penyebabnya.

Jawab :

- Malware : Mirai Variant V3G4 Targets 13 Vulnerabilities to Infect IoT Devices

  Mirai Variant V3G4 adalah salah satu varian dari malware Mirai. Mirai sendiri adalah jenis malware yang biasanya menyerang perangkat Internet of Things (IoT) dan menggunakannya untuk membentuk jaringan zombie atau botnet yang dapat digunakan untuk melakukan serangan Distributed Denial of Service (DDoS).

  Mirai Variant V3G4 merupakan varian Mirai yang terbaru dan diketahui mampu mengeksploitasi kerentanan pada perangkat IoT yang berjalan pada platform ARM dan berbasis kernel Linux. Varian ini mampu menyerang perangkat seperti kamera keamanan, router, dan DVR yang memiliki kelemahan pada protokol Telnet dan SSH.

  Mirai Variant V3G4 dapat menyebar melalui internet dengan mencari perangkat yang memiliki kerentanan dan menginfeksinya dengan cepat. Setelah berhasil memasuki perangkat, malware ini akan mengambil kendali atas perangkat tersebut dan menghubungkannya ke jaringan botnet, sehingga perangkat dapat digunakan untuk melakukan serangan DDoS.

  Pelaku ancaman menargetkan 13 kerentanan eksekusi kode jarak jauh yang memungkinkan mereka menjalankan utilitas khusus untuk mengunduh dan mengeksekusi malware Mirai pada perangkat target. Dampak kerentanan yang ditargetkan FreePBX Elastix (CVE-2012-4869), Gitorious, FRITZ!Box webcams (CVE-2014-9727), Mitel AWC, Geutebruck IP cameras (CVE-2017-5173), Webmin (CVE-2019-15107), Spree Commerce, FLIR Thermal cameras, DrayTek Vigor (CVE-2020-8515 and CVE-2020-15415), Airspan AirSpot (CVE-2022-36267), Atlassian Confluence (CVE-2022-26134), and C-Data Web Management System (CVE-2022-4257). Setelah eksekusi yang berhasil pada perangkat yang rentan, varian Mirai memastikan bahwa hanya satu contoh malware yang berjalan, kemudian mencoba untuk menghentikan proses yang termasuk dalam 'daftar berhenti' yang di-hardcode.

- Ransomware ESXiArgs

  Ransomware ESXiArgs adalah sebuah jenis program ransomware yang dirancang untuk menyerang server VMware vSphere ESXi. Ransomware ini bekerja dengan mengenkripsi file-file penting dan kemudian menuntut pembayaran uang tebusan agar korban dapat memperoleh kembali akses ke data mereka.

  Nama ESXiArgs berasal dari argumen yang digunakan oleh penjahat untuk menjalankan ransomware tersebut pada server ESXi. Ransomware ini dapat menyebar melalui jaringan dengan memanfaatkan kerentanan keamanan pada server ESXi atau melalui serangan phishing yang berhasil.

  Jika server ESXi terinfeksi oleh ransomware ESXiArgs, maka semua mesin virtual yang berjalan di atasnya dapat terkena dampaknya. Korban dapat kehilangan akses ke data penting dan sistem mereka tidak dapat berjalan dengan normal tanpa membayar uang tebusan.

- Malware PoS Prilex

  Prilex adalah jenis malware point-of-sale (PoS) yang digunakan untuk mencuri informasi kartu kredit dan debit dari sistem pembayaran ritel. Malware ini pertama kali ditemukan pada tahun 2014 dan aktif menyebar di Brasil, namun sejak itu juga telah menyebar ke berbagai negara di seluruh dunia.

  Prilex bekerja dengan cara menyusup ke dalam sistem pembayaran ritel melalui jaringan internet atau melalui serangan phishing yang berhasil. Setelah terinstal, Prilex akan memanipulasi perangkat lunak POS untuk mencuri data pembayaran kartu kredit dan debit yang melewati sistem tersebut.

  Prilex menggunakan teknik enkripsi untuk menyimpan data yang dicurinya dan mengirimkan data tersebut ke server komando dan kontrol yang

dikendalikan oleh pelaku kejahatan. Setelah itu, data tersebut dapat digunakan untuk melakukan kegiatan penipuan atau dijual di pasar gelap online.

Selain mencuri data pembayaran, Prilex juga dapat memantau aktivitas penggunaan kartu kredit dan debit secara real-time dan mencuri informasi pengguna seperti nomor PIN, tanggal lahir, dan alamat email.

Malware point-of-sale (PoS) bernama Prilex telah dimodifikasi untuk memblokir transaksi tanpa kontak dalam upaya memaksa pengguna memasukkan kartu kredit mereka ke terminal dan mencuri informasi mereka. pada tahun 2017, Prilex telah berevolusi dari penargetan ATM menjadi malware PoS canggih yang dapat melakukan berbagai aktivitas jahat yang mengarah ke penipuan kartu kredit.

- Trojan : Locky Ransomware

  Locky ransomware adalah jenis program jahat yang menargetkan pengguna komputer untuk mengenkripsi file mereka dan meminta tebusan untuk mendapatkan kunci dekripsi. Nama Locky berasal dari ekstensi file yang ditambahkan ke file yang dienkripsi, yaitu ".locky". Locky ransomware pertama kali muncul pada awal tahun 2016 dan menyebar melalui kampanye spam email yang berisi file dokumen Microsoft Word yang berbahaya. Jika pengguna membuka dokumen ini dan mengaktifkan macros (skrip makro), ransomware akan diunduh dan diinstal pada sistem pengguna.

  Setelah terinstal, Locky akan mulai mengenkripsi file pengguna menggunakan enkripsi AES-128 dan RSA-2048. File-file ini tidak dapat diakses kecuali jika pengguna membayar tebusan dalam bentuk bitcoin atau mata uang digital lainnya. Harga tebusan biasanya berkisar antara beberapa ratus hingga beberapa ribu dolar, dan sering kali berubah-ubah. Locky ransomware juga menggunakan teknik "command-and-control" (C&C) untuk berkomunikasi dengan server jahat, yang dapat digunakan untuk mengambil perintah tambahan dan mengirimkan data yang dikumpulkan.

Locky ransomware telah menyebar luas dan menimbulkan kerugian finansial yang besar bagi banyak korban. Meskipun ada beberapa alat yang tersedia untuk membantu memulihkan file yang dienkripsi tanpa membayar tebusan, tidak ada jaminan bahwa file tersebut dapat sepenuhnya dipulihkan. Oleh karena itu, penting untuk selalu mengambil tindakan pencegahan yang tepat, seperti tidak membuka lampiran email yang mencurigakan dan menginstal perangkat lunak antivirus yang kuat.

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 : Malware PoS Prilex adalah program jahat yang dirancang untuk mencuri informasi pembayaran dari perangkat penjualan ritel (PoS) atau terminal pembayaran kartu kredit. Setelah terinstal pada perangkat PoS, malware Prilex akan mencuri data kartu kredit atau debit yang diambil oleh terminal pembayaran tersebut. Informasi yang dicuri meliputi nomor kartu, tanggal kadaluarsa, dan kode keamanan kartu (CVV). Malware Prilex juga dapat mengambil informasi PIN (Personal Identification Number) jika perangkat PoS tersebut memiliki keyboard numerik yang terpasang.

Malware PoS Prilex dapat menyebar melalui beberapa cara, termasuk:

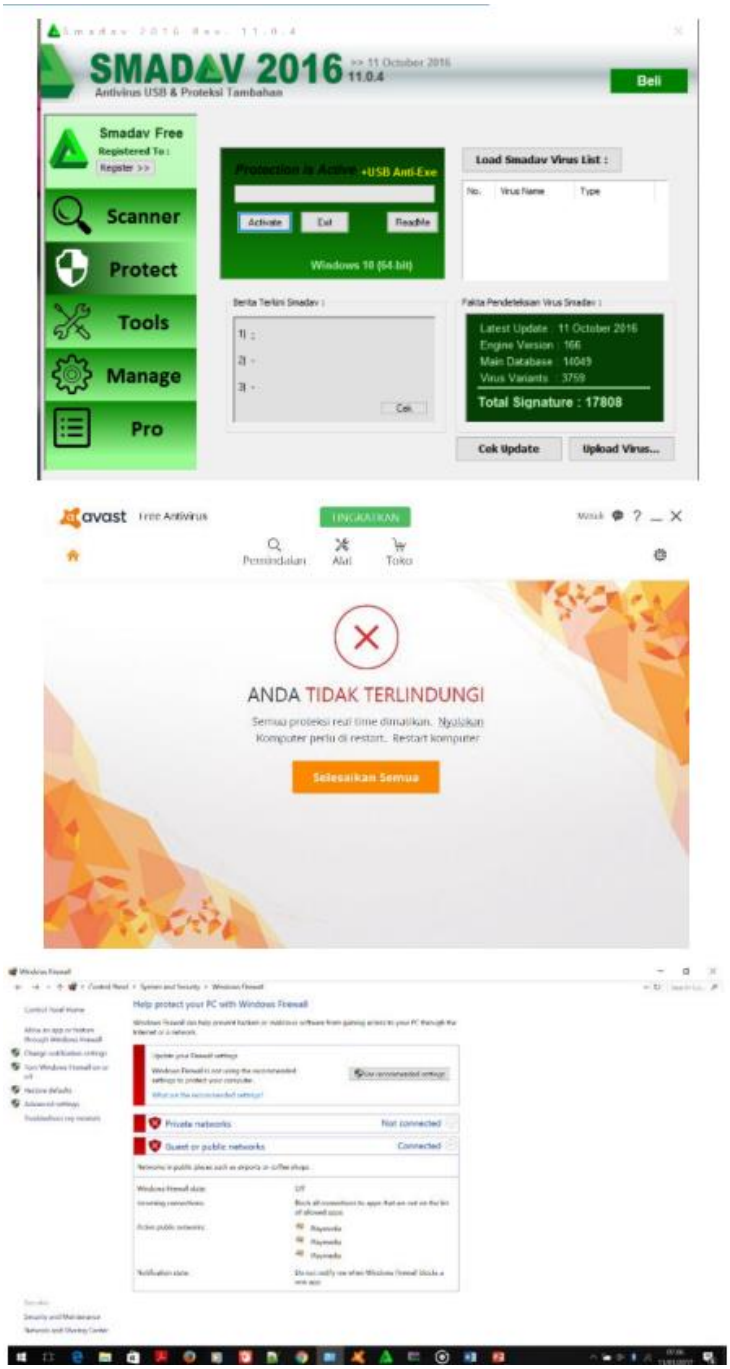
- Eksploitasi Kerentanan: Malware Prilex dapat menyebar melalui kerentanan dalam perangkat lunak atau sistem operasi pada perangkat PoS. Penjahat dapat mengeksploitasi kerentanan ini untuk menginstal malware pada perangkat PoS tanpa sepengetahuan pengguna.
- Serangan Phishing: Penjahat dapat menyebar malware Prilex melalui email phishing atau pesan teks yang menipu korban untuk mengklik tautan atau mengunduh lampiran berbahaya. Tautan atau lampiran tersebut dapat menginstal malware Prilex pada perangkat PoS korban.
- Infeksi melalui USB: Malware Prilex juga dapat menyebar melalui perangkat USB yang terinfeksi. Penjahat dapat menyebarkan malware Prilex melalui perangkat USB yang disisipkan pada perangkat PoS atau sistem terkait.

- Jaringan yang tidak aman: Perangkat PoS yang terhubung ke jaringan yang tidak aman atau tidak terlindungi dapat menjadi sasaran penyerangan oleh malware Prilex. Penjahat dapat memindai jaringan untuk mencari celah keamanan dan memanfaatkannya untuk menyebar malware Prilex.

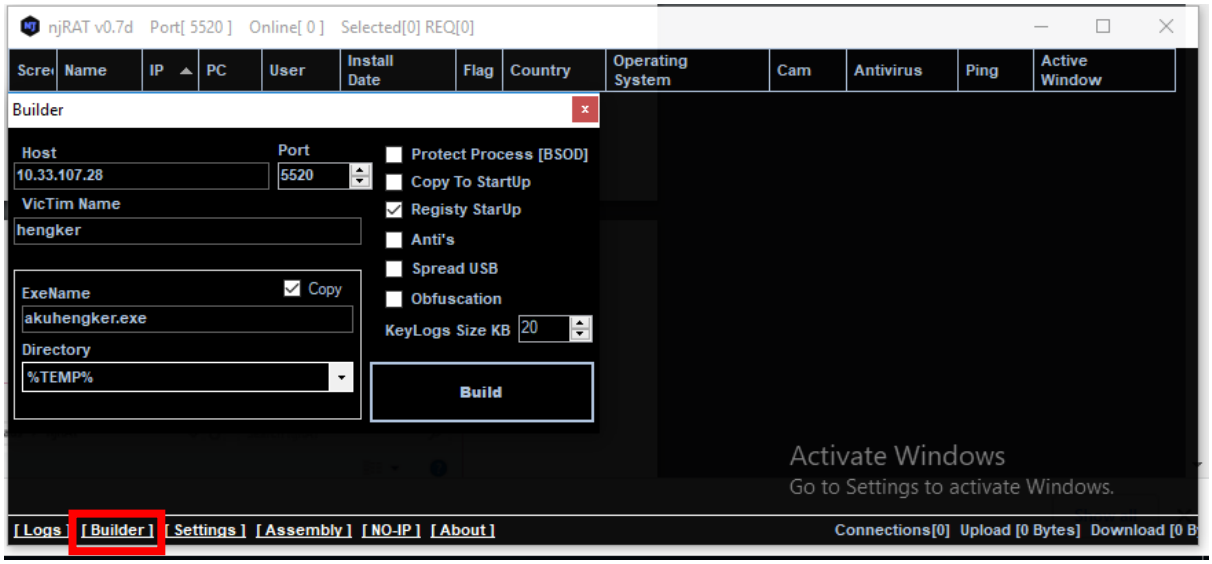
Data yang dicuri oleh malware Prilex kemudian dikirim ke server jahat yang dikelola oleh para penjahat. Data ini dapat digunakan untuk membuat salinan kartu kredit atau debit yang valid atau dijual ke pasar gelap daring.

**Unit NjRAT**

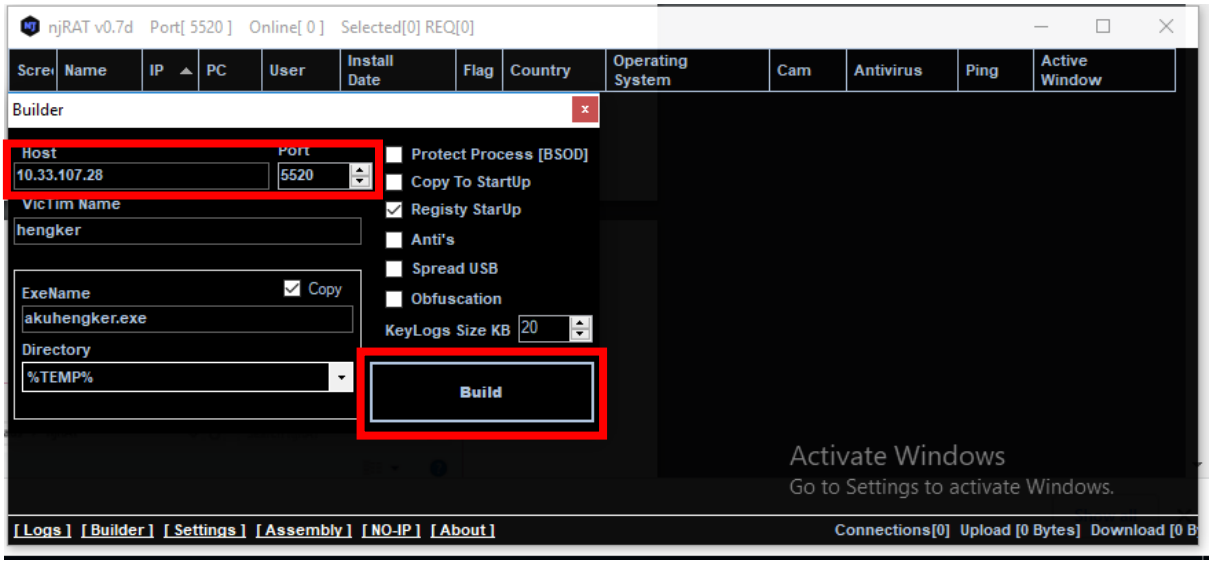
1. Gunakan OS Windows 10 pada komputer yang akan dijadikan target, kemudian mematikan semua antivirus dan firewall pada kedua komputer yang digunakan untuk memakai aplikasi njrat ini.

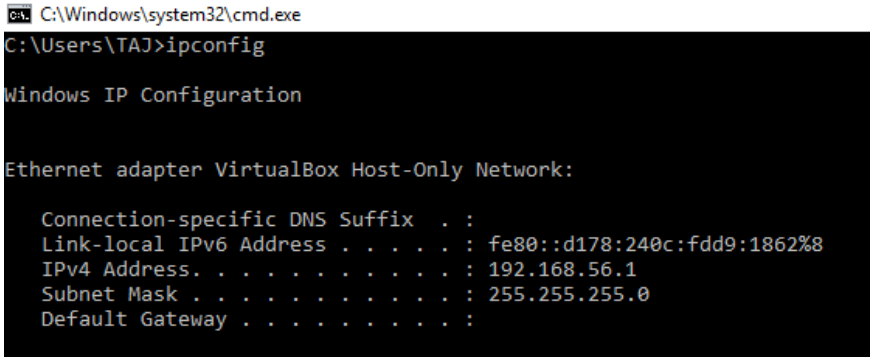



2. Download dan ekstrak aplikasi NJRAT kemudian run aplikasi NJRAT pada komputer host. Setelah itu jalankan aplikasi NjRAT dan klik builder.

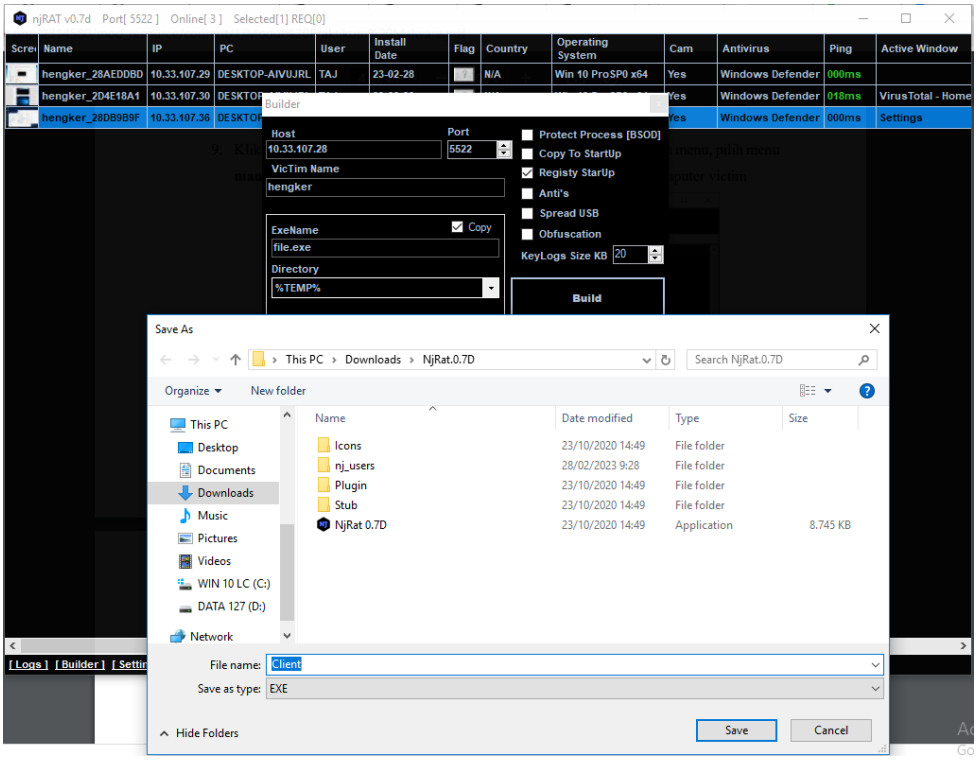



3. Masukkan IP Address host pada kolom host dan port “5520”, kemudian klik tombol build.

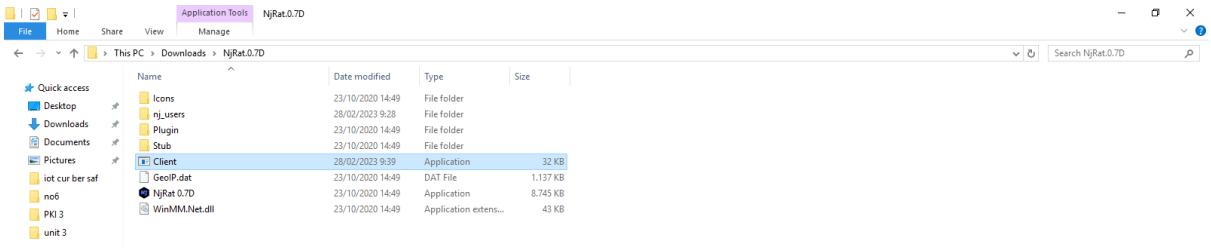


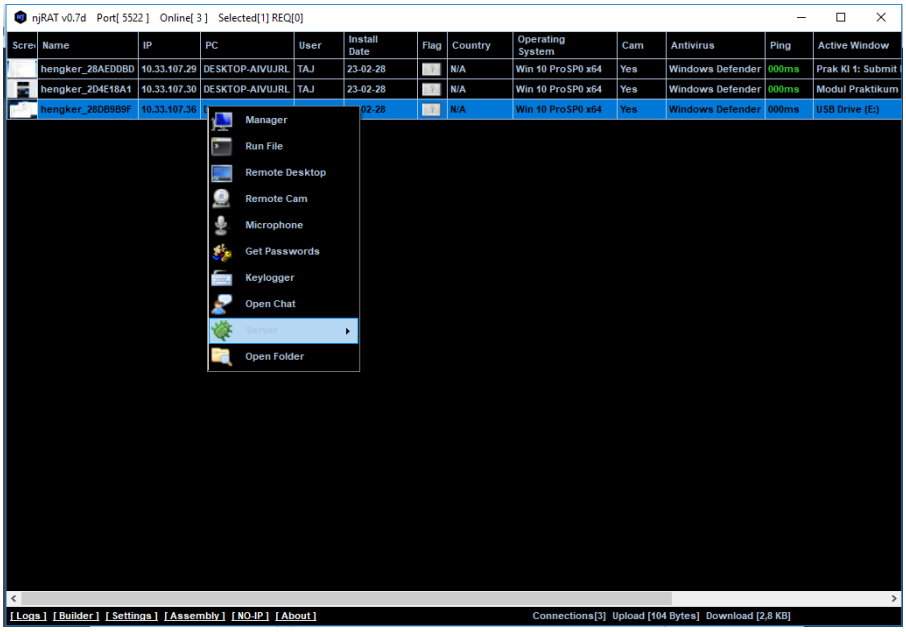

4. Simpan aplikasi hasil build.



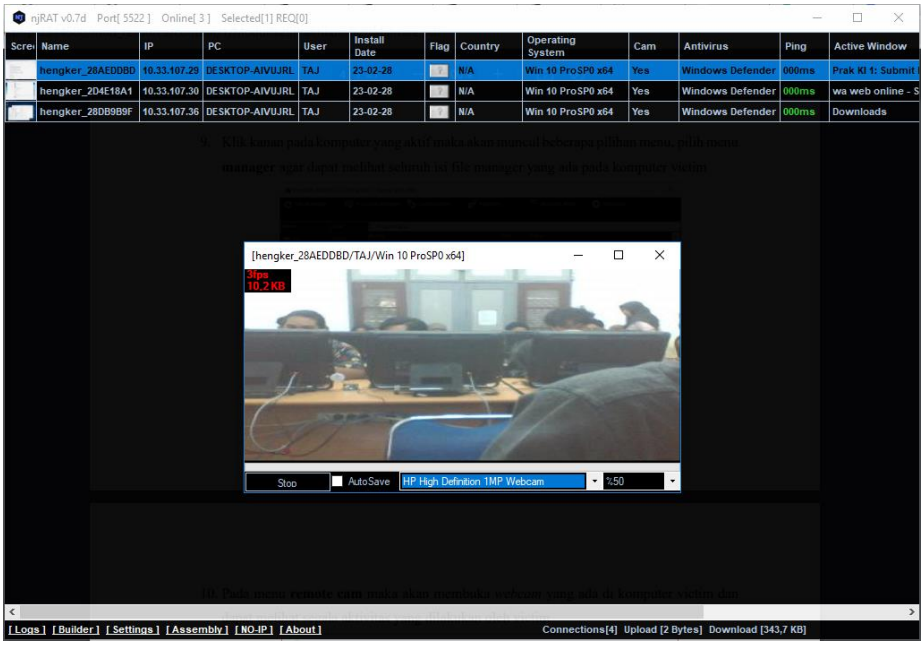

5. Coppy kan file .exe ke komputer target dan jalankan file .exe.



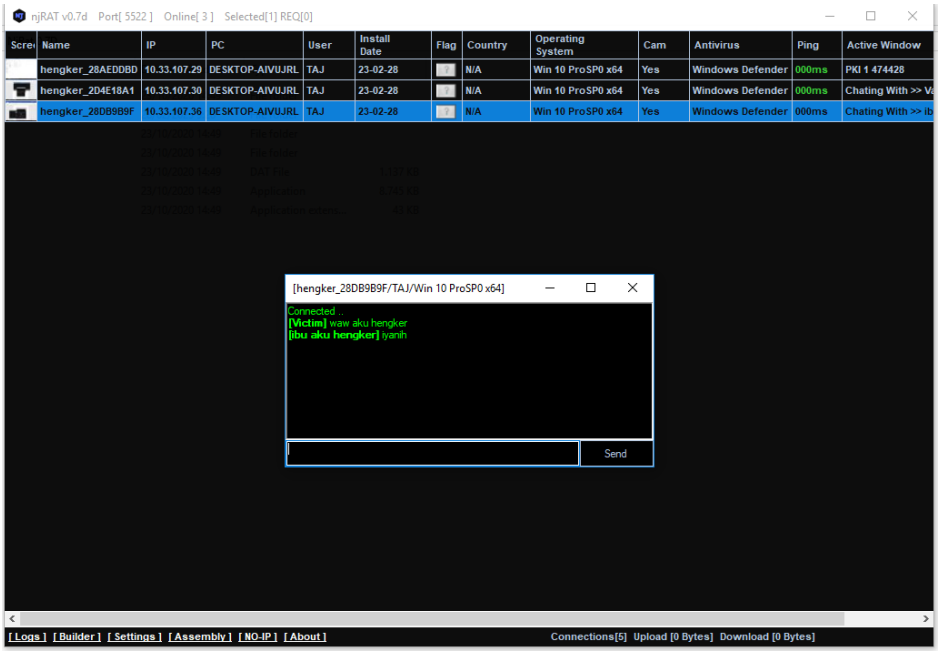

6. Ketika sudah terpasang pada komputer target, NJRAT pada host akan mendeteksi komputer target. Dan terdapat banyak sekali tools yang dapat dilakukan pada komputer target dengan klik kanan pada komputer target.



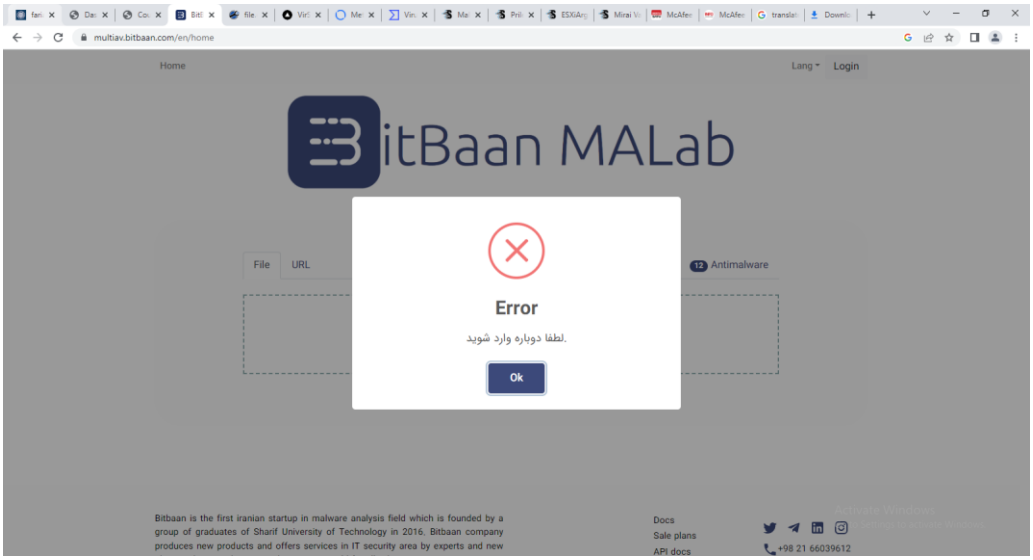

7. Hasil saat menggunakan tools Remote Cam dimana computer target akan menyala dan komputer host dapat memonitornya.



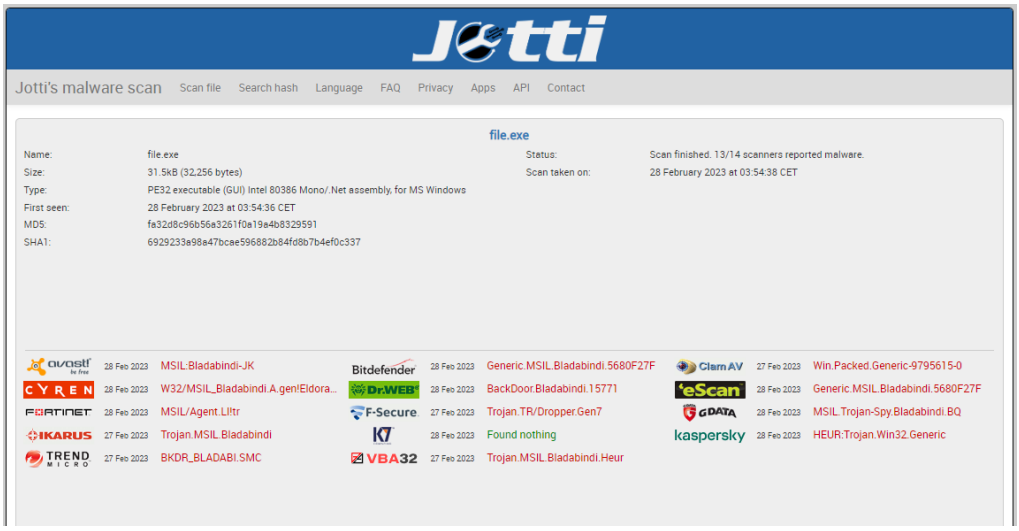

8. Hasil saat menggunakan tools open chat dimana komputer host dan komputer target dapat berkomunikasi lewat chat dan komputer target tidak dapat menonaktifkan fitur chat secara paksa.

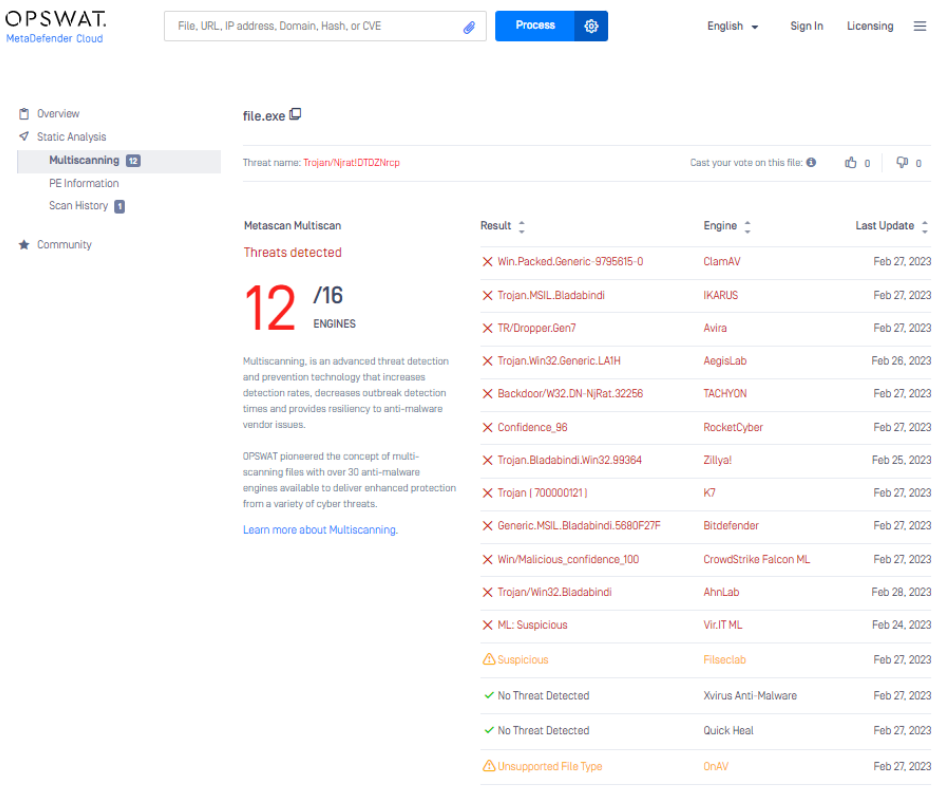



9. Hasil dari analisis malware dengan metode osint.

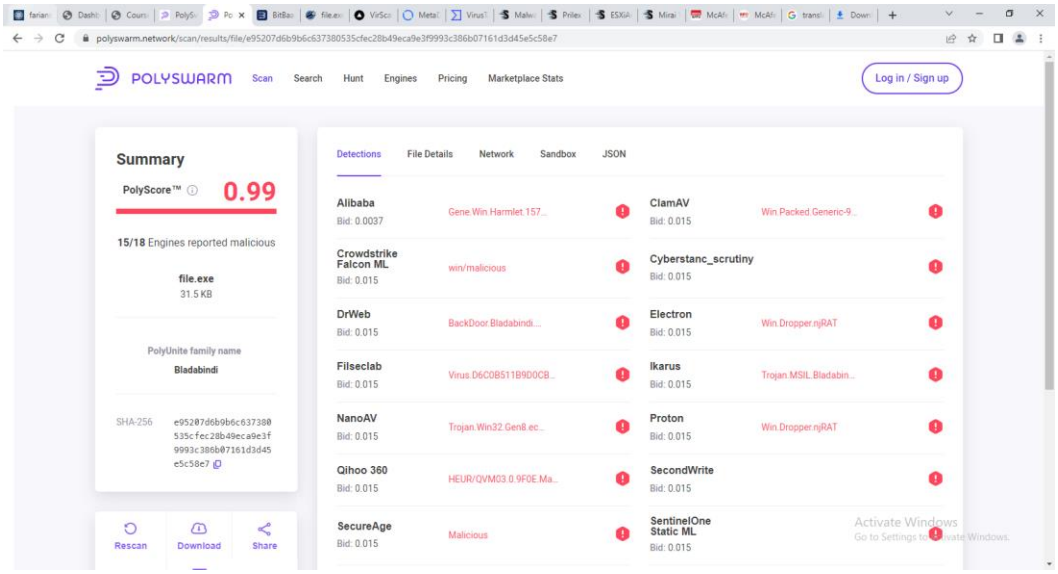



BitBaan MALab

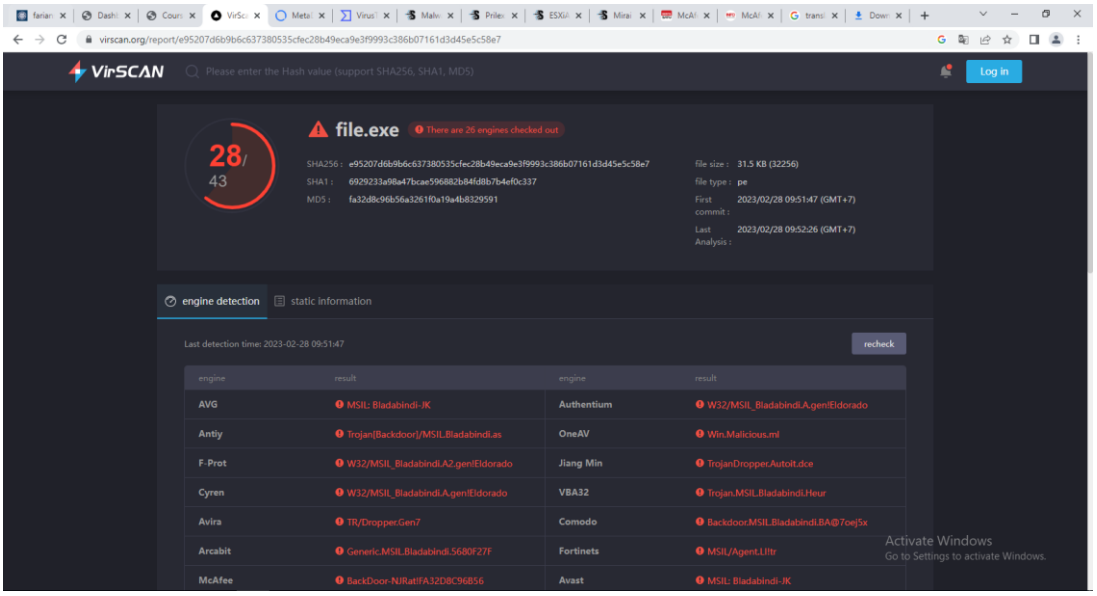


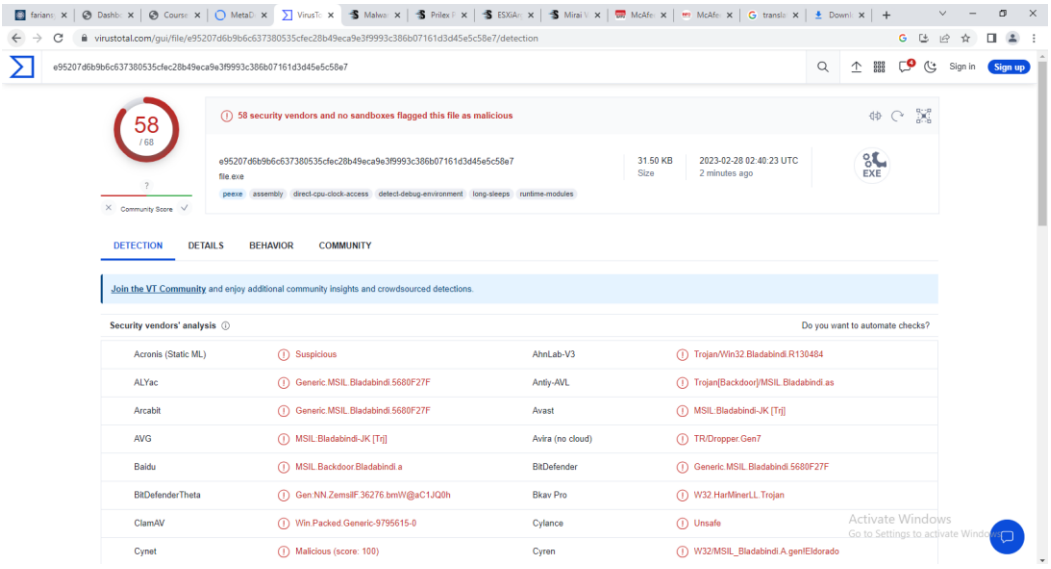

OPSWAT. (MetaDefender Cloud)




POLYSWARM




VirSCAN




Virustotal

## D. Analisis

Pada praktikum Keamanan Informasi 1 petemuan 3 membahas mengenai Malware dan membuat Malware Trojan menggunakan NjRAT. Malware adalah singkatan dari malicious software (perangkat lunak berbahaya). Malware adalah program komputer yang dirancang untuk merusak atau memata-matai sistem komputer tanpa izin atau pengetahuan pengguna. Malware dapat merusak, mencuri, atau menghancurkan data, memperlemah sistem keamanan, mencuri informasi pribadi atau keuangan, dan dapat mengakibatkan kerugian finansial dan kerugian lainnya bagi korban yang terkena. Sedangkan 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

.

Pada unit 4 diperintahkan mencari tau tentang malware dan contoh jenis malware seperti : Ransomware, Trojan, Hoax, Adware, Malware, PUP, Exploit, Exploit Kit dan Kerentanan. Dan juga mencari tahu contoh kasus melaui beberapa situs website yang khusus membahas tentang perkembangan security dan malware. Disini saya mendapat contoh kasus malware berasal dari situs web : https://www.securityweek.com/category/malware-cyber-threats/. Di web tersebut banyak sekali contoh dari kasus malware yang ter update serta pencegahannya.

Pada unit NjRAT disini membuat sebuah malware dengan jenis trojan dimana Remote Access Trojan ini adalah sebuah trojan yang kita buat dan infeksikan ke korban, yang mana setelah trojan berjalan, kita punya hak akses dan kontrol penuh terhadap komputer infeksi tersebut. Aplikasi yang digunakan adalah NjRAT dimana perlu mematikan antivirus dan windows firewall pada komputer host maupun komputer target. Setelah mengirim file .exe ke target dan target membuka file tersebut maka secara otomatis terdapat nama komputer target pada aplikasi NjRAT. Pada aplikasi tersebut dapat dilakukan :

- Remote Desktop - NjRAT memungkinkan pengguna untuk mengendalikan sistem yang terinfeksi dari jarak jauh melalui remote desktop.
- File Manager - NjRAT memungkinkan pengguna untuk mengakses dan mengelola file dan folder pada sistem yang terinfeksi.
- Keylogger - NjRAT dapat merekam setiap kunci yang ditekan pada keyboard pada sistem yang terinfeksi, sehingga memungkinkan penyerang untuk mencuri informasi sensitif seperti username dan password.
- Password Stealer - NjRAT dapat mencuri kata sandi yang tersimpan pada browser web dan klien email.
- Webcam dan Mikrofon - NjRAT dapat mengambil alih kontrol webcam dan mikrofon pada sistem yang terinfeksi, sehingga memungkinkan penyerang untuk merekam video dan audio.
- Screen Capture - NjRAT dapat merekam layar sistem yang terinfeksi, sehingga memungkinkan penyerang untuk melihat aktivitas yang sedang dilakukan pada sistem tersebut.

- Remote Shell - NjRAT dapat memberikan akses shell jarak jauh pada sistem yang terinfeksi, sehingga memungkinkan penyerang untuk menjalankan perintah pada sistem tersebut.
- Denial of Service (DoS) - NjRAT dapat digunakan untuk melakukan serangan DoS pada sistem yang terinfeksi.
- Registry Editor - NjRAT memungkinkan pengguna untuk mengakses dan mengelola registri pada sistem yang terinfeksi.
- System Information - NjRAT dapat memberikan informasi tentang sistem yang terinfeksi, termasuk versi sistem operasi, perangkat keras, dan perangkat lunak yang terinstal.

Dan kemudian melakukan analisis file .exe yang merupakan malware menggunakan metode OSINT. OSINT (Open-Source Intelligence) adalah metode pengumpulan informasi yang memanfaatkan sumber-sumber informasi yang tersedia secara publik, seperti situs web, media sosial, basis data publik, dan sumber-sumber informasi publik lainnya. Metode OSINT digunakan untuk mengumpulkan informasi tentang individu, organisasi, atau kejadian tertentu untuk tujuan analisis atau investigasi. Disini tools yang digunakan antara lain : VirusTotal, OPSWAT(Meta Defender), VirSCAN, Jotti, Bitbaan MaLab, PolySwarm. Dan berikut data yang didapat dari analisis metode OSINT pada file NjRAT.

| No. | OSINTs | File NjRAT .exe |
|---|---|---|
| 1. | BitBaan | - |
| 2. | Jotti | 13/14 |
| 3. | OPSWAT (MetaDefender | 12/16 |
| 4. | POLYSWARM | 15/18 |
| 5. | VirusTotal | 58/68 |
| 6. | VirSCAN | 28/43 |

Terlihat bahwa tools yang bagus adalah Jotti dan POLYSWARM dimana perbandingan nya mendekati 1 sedangkan yang kurang bagus adalah VirSCAN dimana dari 43 engine yang digunakan untuk scan virus .exe hanya 28 yang mendeteksi virus tersebut.

## E. Kesimpulan

Berdasarkan data diatas dapat disimpulkan bahwa malware adalah jenis perangkat lunak berbahaya yang dirancang untuk menyebabkan kerusakan atau mencuri informasi dari sistem yang terinfeksi. Malware dapat menyebar melalui berbagai cara, seperti email spam, situs web yang tidak aman, atau melalui drive-by-download. Ada berbagai jenis malware, termasuk virus, worm, trojan, ransomware, dan spyware, yang masing-masing memiliki tujuan dan cara kerja yang berbeda-beda.

Pencegahan terbaik terhadap malware adalah dengan menginstal dan menjalankan perangkat lunak keamanan yang andal, seperti antivirus dan firewall. Selain itu, pengguna juga harus berhati-hati dalam membuka email dan mengakses situs web yang mencurigakan, serta melakukan tindakan keamanan yang diperlukan seperti mengubah password secara berkala dan melakukan backup data secara rutin.

## F. Daftar Pustaka


1. Ariyandi, S. (1970, January 1). *NJRAT, tool Untuk Mengendalikan Komputer Orang Lain*. NjRAT, Tool untuk Mengendalikan Komputer Orang Lain. Retrieved March 6, 2023, from http://itpens.blogspot.com/2016/06/njrat-tool-untuk-mengendalikan-komputer.html
2. Hosting, R. J. (2022, July 12). *Apa Itu trojan, Pengertian, Contoh Dan Cara Mengatasinya*. Blog Jagoan Hosting | Tutorial Website & Web Hosting Indonesia. Retrieved March 6, 2023, from https://www.jagoanhosting.com/blog/trojan-adalah/#:~:text=Contoh%20Trojan%20Horse%20yang%20paling,ini%20diketahui%20pernah%20membajak%20Amazon.
3. Novel, M. (2022, June 11). *Apa ITU OSINT (Opent Source Intelligence) ? - CSIRT UMM*. Apa itu OSINT (Opent Source Intelligence)? Retrieved March 6, 2023, from https://csirt.umm.ac.id/2022/06/apa-itu-osint-opent-source-intelligence/