LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1

Pertemuan 3 – Analisis *Malware*

DISUSUN OLEH

Nama	: Sofiyanatul Munawaroh
NIM	: 21/474781/SV/19035
Hari, Tanggal	: Selasa, 28 Februari 2023
Kelas	: RI4AA

LABORATORIUM PERANGKAT KERAS DAN LUNAK

PROGRAM SARJANA TERAPAN (DIV) TEKNOLOGI

REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

2023

Praktikum Keamanan Informasi 1

Pertemuan 3 – Analisis *Malware*

I. Tujuan

- Meneliti dan menganalisis *malware.*

II. Latar Belakang

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*.

Salah satu jenis *malware* yaitu trojan, yang akan kita praktikkan pada pertemuan ini dengan sistem *remote access. 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 di-*upload* 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.

NjRAT adalah salah satu *tools hacking* untuk OS windows yang digunakan untuk me-*remote* PC satu dengan PC lain.

RAT adalah singkatan dari *Remote Administrator Tool* yang digunakan untuk menghubungkan dan mengatur satu atau lebih komputer dengan berbagai kemampuan seperti:

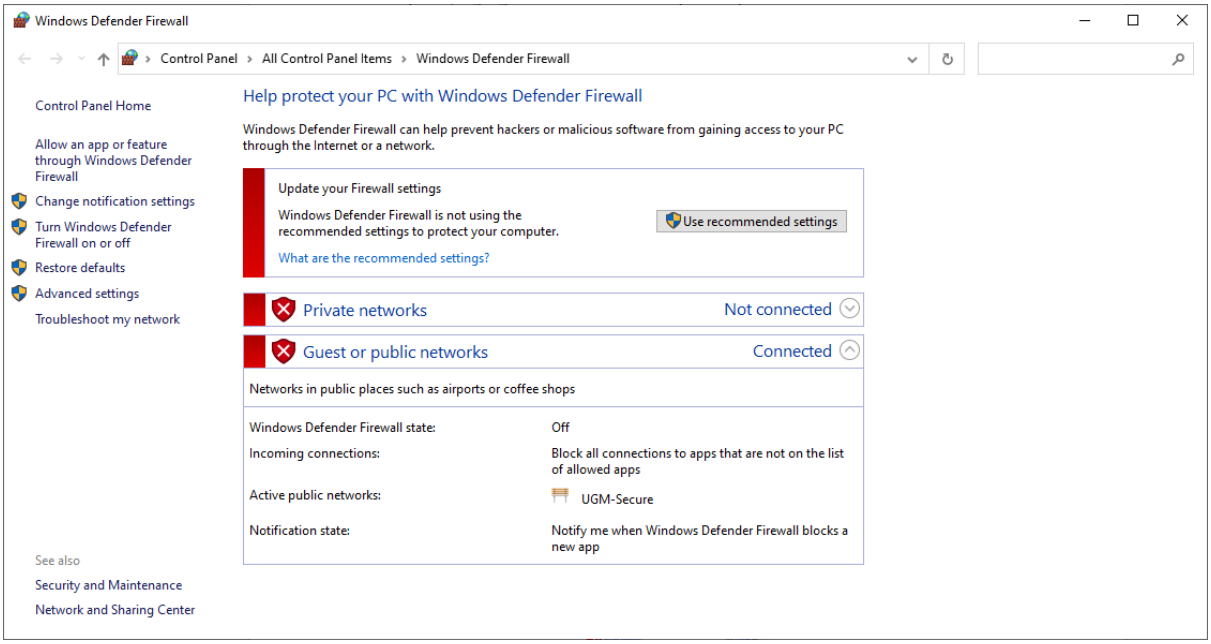
- *Screen/camera capture* atau *control.*
- *File management* (*download/upload/execute/*dll.)
- *Shell control* (CMD *control*).
- *Computer control (power off/on/log off).*
- *Registry management (query/add/delete/modify).*
- *Password management.*

III. Alat dan Bahan

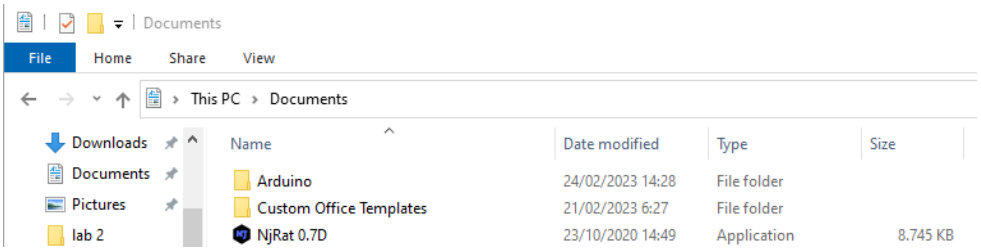
- PC/Laptop.
- *Software* NJRAT.
- Koneksi internet.

IV. Instruksi Kerja

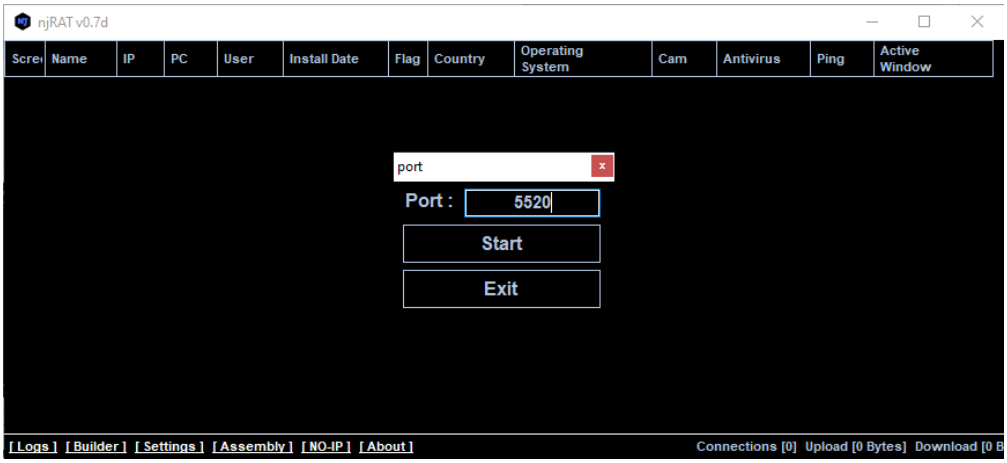
1. Menggunakan mesin pencari favorit Anda, lakukan pencarian untuk *malware* terbaru. Selama pencarian Anda, pilih empat contoh *malware,* masing-masing dari jenis *malware* yang berbeda, dan bersiaplah untuk membahas detail tentang apa yang dilakukan masing-masing, bagaimana masing-masing ditransmisikan, dan dampak masing-masing penyebabnya.
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. Selanjutnya, buka modul praktikum *malware* NJRAT.
4. Matikan semua *antivirus* dan *firewall* pada kedua komputer yang digunakan untuk memakai aplikasi njrat ini.



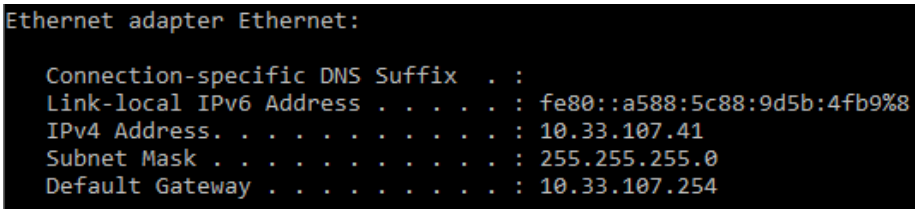
5. *Download* dan ekstrak aplikasi NJRAT kemudian *run* aplikasi NJRAT pada komputer *host*.



6. Masukkan *port* yang ingin digunakan yaitu 5520.

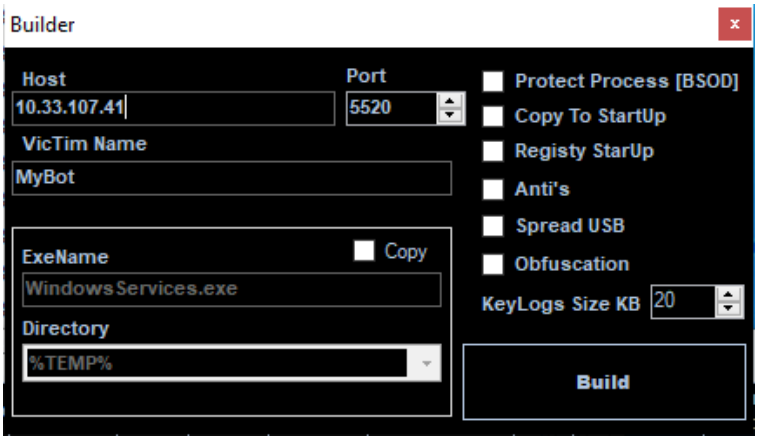


7. Sebelumnya, cek IP *Address* milik *host* terlebih dahulu. IP ini nantinya akan digunakan oleh NJRAT, dan pastikan juga komputer *victim* berada pada satu jaringan.

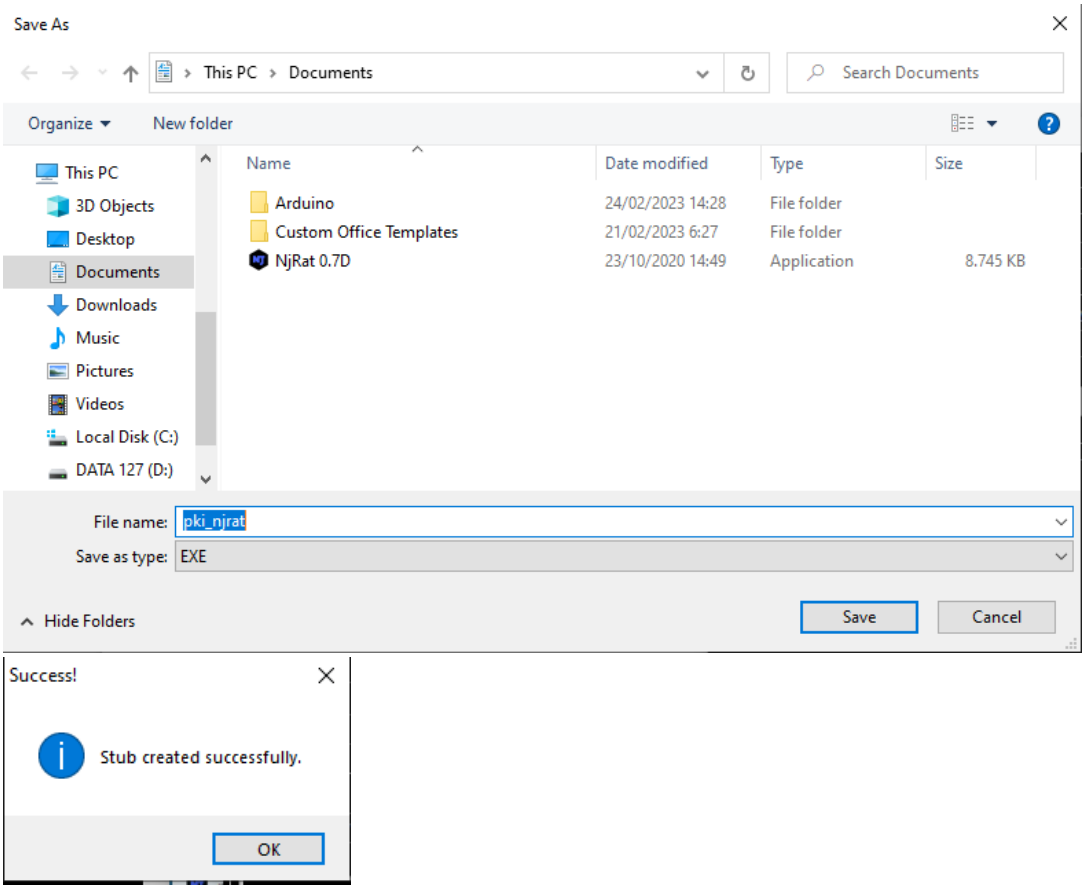


8. Buat aplikasi yang akan dipasang pada komputer *victim*. Masukkan IP *Address host* pada kolom *host* dan *port* yang sesuai dengan yang kita tentukan tadi pada awal

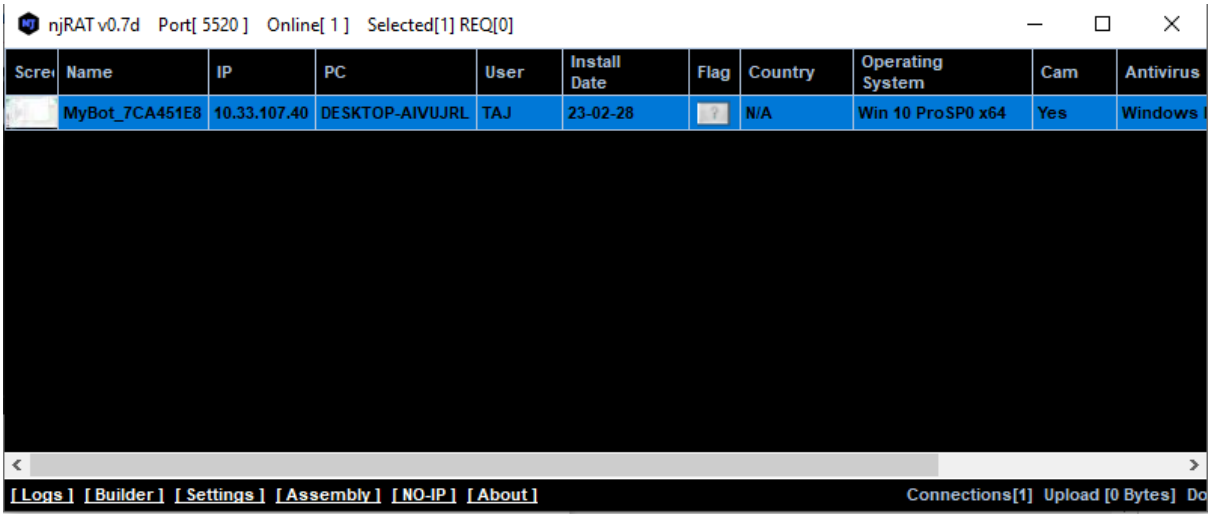
membuka aplikasi NJRAT agar dapat diakses oleh komputer nanti, kemudian klik tombol *build*.



9. Simpan aplikasi hasil *build*.



10. Kemudian, *copy*-kan aplikasi **pki_njrat.exe** yang telah kita buat ke dalam komputer *victim*. Pada komputer *victim* jalankan aplikasi tersebut. Ketika sudah terpasang pada komputer *victim*, NJRAT pada *host* akan mendeteksi komputer *victim.*



V. Hasil dan Pembahasan

a. Analisis *Anatomy Malware*

1. Contoh-Contoh *Malware*

- ***Ransomware* Locky**

  Pada tahun 2016, menurut informasi yang dikeluarkan oleh perusahaan antivirus Eset, Locky merupakan jenis *malware* terbaru yang memanfaatkan email dan menyamarkan diri menjadi *invoice* perusahaan yang berisi *file* Microsoft Word, apabila diklik maka hal buruk akan terjadi pada sistem komputer dan menyebabkan kerusakan fatal.

- ***Backdoor***

  Dikutip dari sitelock.com, *backdoor attack* adalah salah satu jenis *malware* yang dapat membukakan akses ke dalam suatu situs *web* atau sistem jaringan komputer secara tidak sah. Para peretas atau penjahat siber memasang *malware* melalui titik masuk yang tidak aman, seperti *plug-in* atau kolom *input* yang sudah usang.

- ***Adware***

  Adware adalah perangkat lunak atau *software* yang mengandung *pop up* iklan dan muncul pada perangkat yang menginstalnya, baik itu di komputer maupun perangkat *mobile*. Kepanjangan dari *adware* sendiri yaitu *advertising supported software*.

- ***Worm***

  Cacing komputer (Inggris: *worm*) dalam keamanan komputer, adalah sebuah program komputer yang dapat menggandakan dirinya secara sendiri dalam sistem komputer. Sebuah *worm* dapat menggandakan dirinya dengan memanfaatkan jaringan (LAN/WAN/Internet) tanpa perlu campur tangan dari *user* itu sendiri.

2. Analisis *Malware* "*Worm"*

Worm tidak seperti virus komputer biasa, yang menggandakan dirinya dengan cara menyisipkan program dirinya pada program yang ada dalam

komputer tersebut, tapi *worm* memanfaatkan celah keamanaan yang memang terbuka atau lebih dikenal dengan sebutan *vulnerability*.

Beberapa *worm* juga menghabiskan *bandwidth* yang tersedia. *Worm* merupakan evolusi dari virus komputer. Hanya ada satu cara untuk mengatasi *worm* yaitu dengan menutup celah keamanan yang terbuka tersebut, dengan cara meng-*update patch* atau *Service Pack* dari *operating* sistem yang digunakan dengan *patch* atau *Service Pack* yang paling terbaru.

Lima komponen yang umum dimiliki oleh *worms* adalah sebagai berikut:

1) *Reconnaissance* : bertugas untuk merintis jalannya penyebaran pada jaringan. Komponen ini memastikan titik-titik mana saja pada jaringan yang dapat diinfeksi olehnya.
2) *Attack* : bertugas untuk melancarkan serangan pada target *node* yang telah teridentifikasi.
3) *Communications* : membuat tiap *node* yang terinfeksi pada jaringan dapat saling berkomunikasi.
4) *Command* : suatu antar muka agar setiap *worms* dapat mengeluarkan perintah (*command*) pada *worms* di titik lain lain.
5) *Intelligent* : komponen cerdas yang mampu memberikan informasi bagaimana karakteristik keadaan *worms* di titik lain pada jaringan.

Berbeda halnya dengan virus, *worm* tidak memiliki kemampuan merusak sistem, *worm* tidak bisa merusak data atau *file* sistem. *Worm* bertingkah hanya sebagai parasit yang tidak secara langsung merusak sistem komputer. Namun jika *worm* dibiarkan maka lambat laun komputer pun akan mengalami penurunan dalam hal kinerja, bahkan karena terus menerus memaksa komputer untuk bekerja ekstra, maka komputer pun akan mengalami kerusakan.

Worm juga berbeda dengan virus dalam hal cara penyebaran atau cara menginpeksi korbannya. Jika virus biasanya memanfaatkan program lain dengan menyisipkan dirinya sendiri pada program tersebut, maka *worm* tidak perlu bantuan program lain untuk menyusup ke sebuah sistem.

Worm memanfaatkan jaringan komputer untuk menyusup ke komputer lain yang terhubung pada jaringan tersebut. Pertama kali *worm* menyusup ke sebuah sistem ialah dengan memanfaatkan celah keamaan atau lebih populer dengan nama *vulnerability*.

Efek dari *worm* pada sistem operasi akan membuat komputer terasa lambat karena dianggap komputer sedang melakukan aktivitas berat, juga pada sistem jaringan komputer maka akan terasa konektivitas jaringan lambat karena *worm* bekerja memenuhi akses jaringan tersebut.

Beberapa program *worm* yang telah diketahui dan cukup populer, diantaranya adalah ADMworm, Code Red, LoveLetter, Nimda, dan SQL-Slammer.

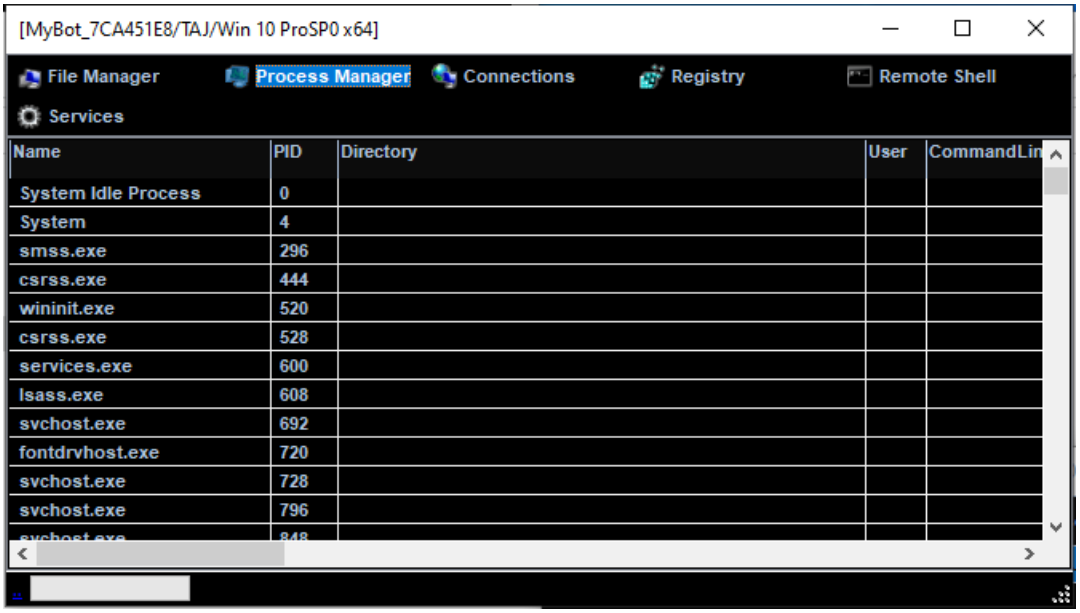
b. Analisis Praktikum *Malware* NJRAT

Pada praktikum ini, diminta untuk *developing malware* menggunakan NJRAT. Agar *software* NJRAT dapat dijalankan maka perlu mematikan *windows firewall defender* dan *antivirus* terlebih dahulu. Jika *windows security* tidak dimatikan, maka windows akan mendeteksi adanya *software* berbahaya yaitu *software* NJRAT, sehingga *software* tidak dapat di-*download* apalagi diinstal.

NJRAT sendiri merupakan salah satu *malware* sejenis Trojan yang menginfeksi komputer *victim* melalui instalasi program. Ketika *malware* terpasang pada PC, maka segala bentuk kegiatan PC *victim* dapat di-*monitoring* atau dikendalikan melalui PC *host* yang berada pada satu jaringan melalui akses IP dan *port* yang telah ditentukan di awal.

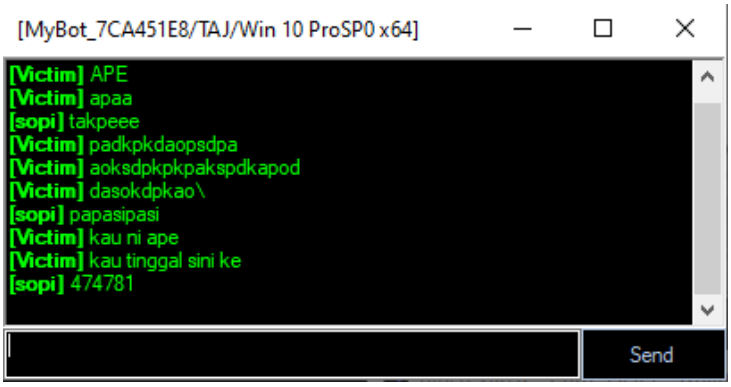
Setelah *software* NJRAT telah diinstal, kemudian dilakukan *build* aplikasi yang akan diinstal di PC *victim.* Sebelum itu, masukan IP *Address* dari PC *host* yang digunakan serta *port* yang ingin digunakan. Pastikan juga *host* ada dalam satu jaringan dengan komputer korban, karena pengujian hanya dilakukan di dalam jaringan lokal. Setelah *file* aplikasi berhasil dibuat, jalankan aplikasi tersebut di komputer korban dan pastikan *host* telah mendeteksi komputer korban.

Kemudian lakukan beberapa pengujian seperti *remote camera, remote file manager,* dan *open chat.*



Pada *remote file manager, host* dapat melihat seluruh isi *file manager* yang ada pada komputer korban.

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

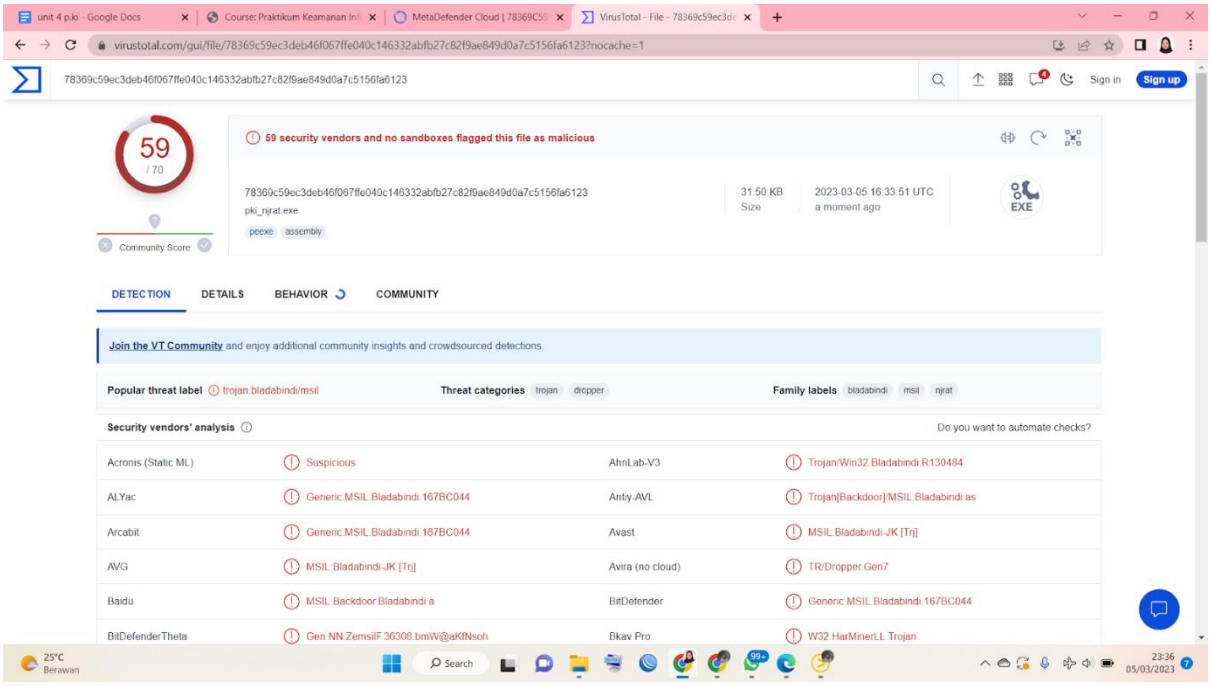


Pada pilihan *chat message*, kita dapat mengirimkan pesan ke layar *desktop* komputer *victim*, dan *user* komputer dapat melakukan balasan tanpa bisa menutup *chat.*

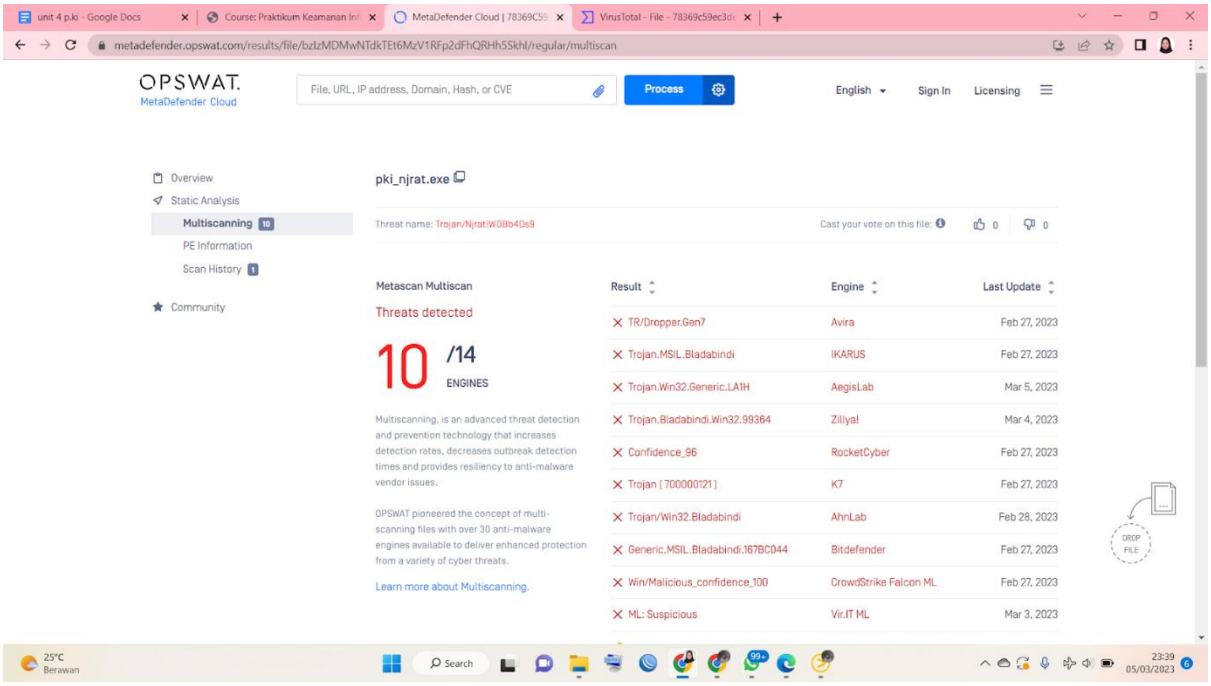
c. Analisis *Malware* dengan Metode OSINT

Hasil *Scanning* dengan Metode OSINT

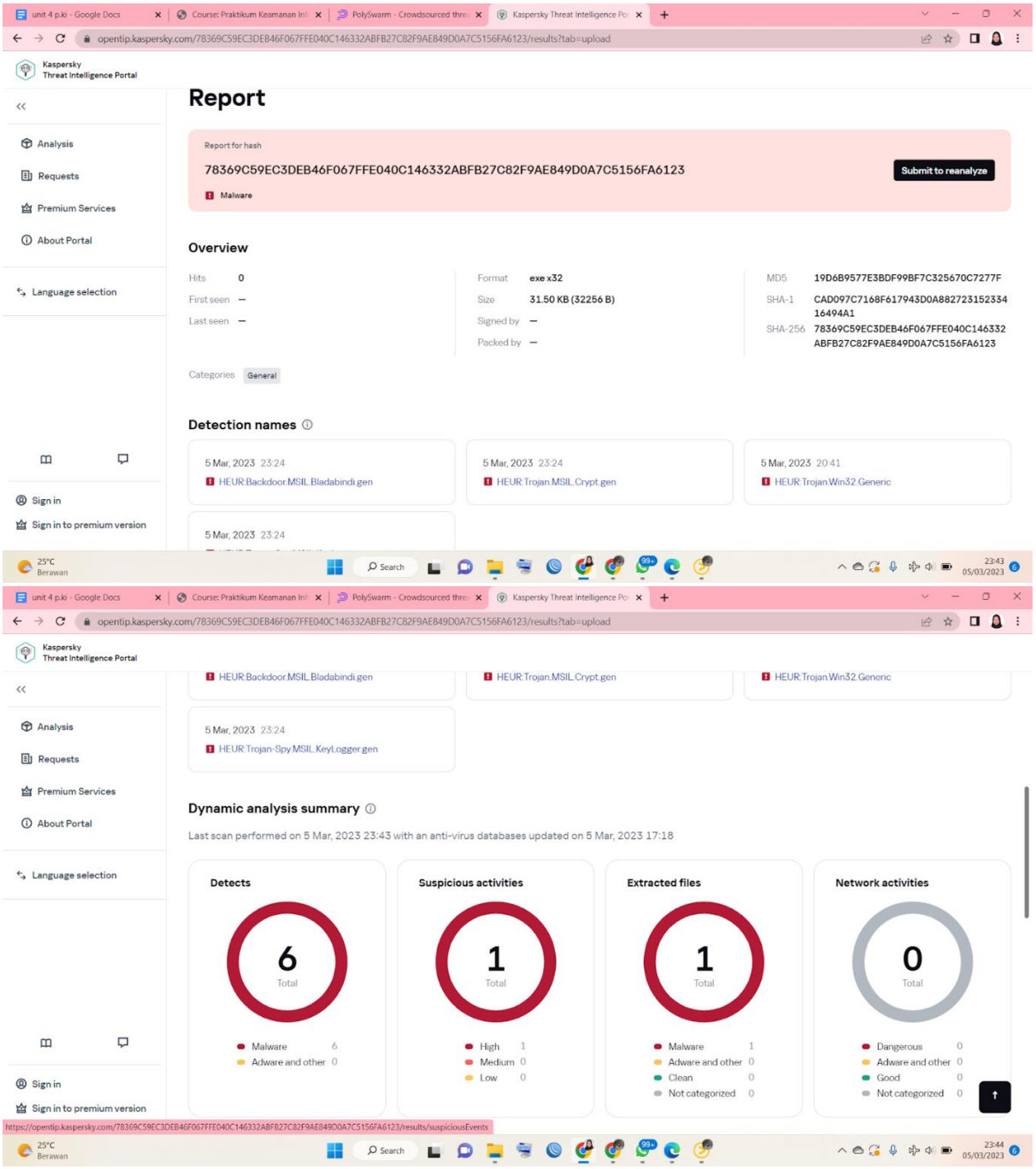
1) VirusTotal

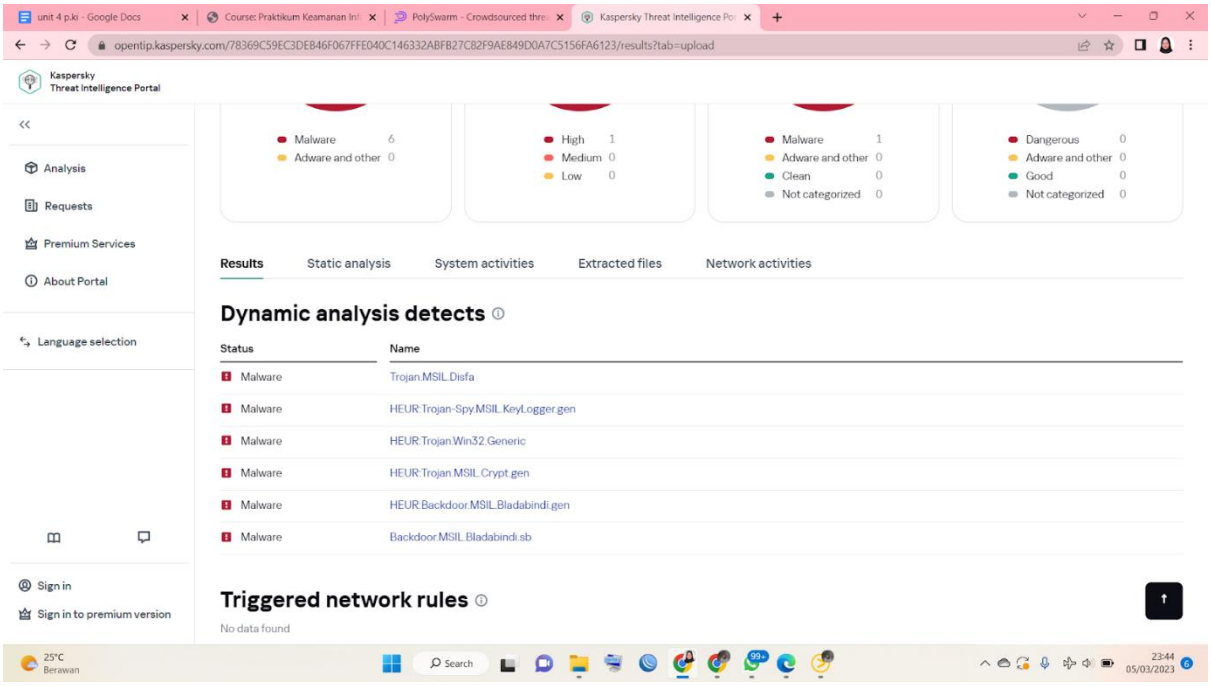


2) OPSWAT (Meta Defender)

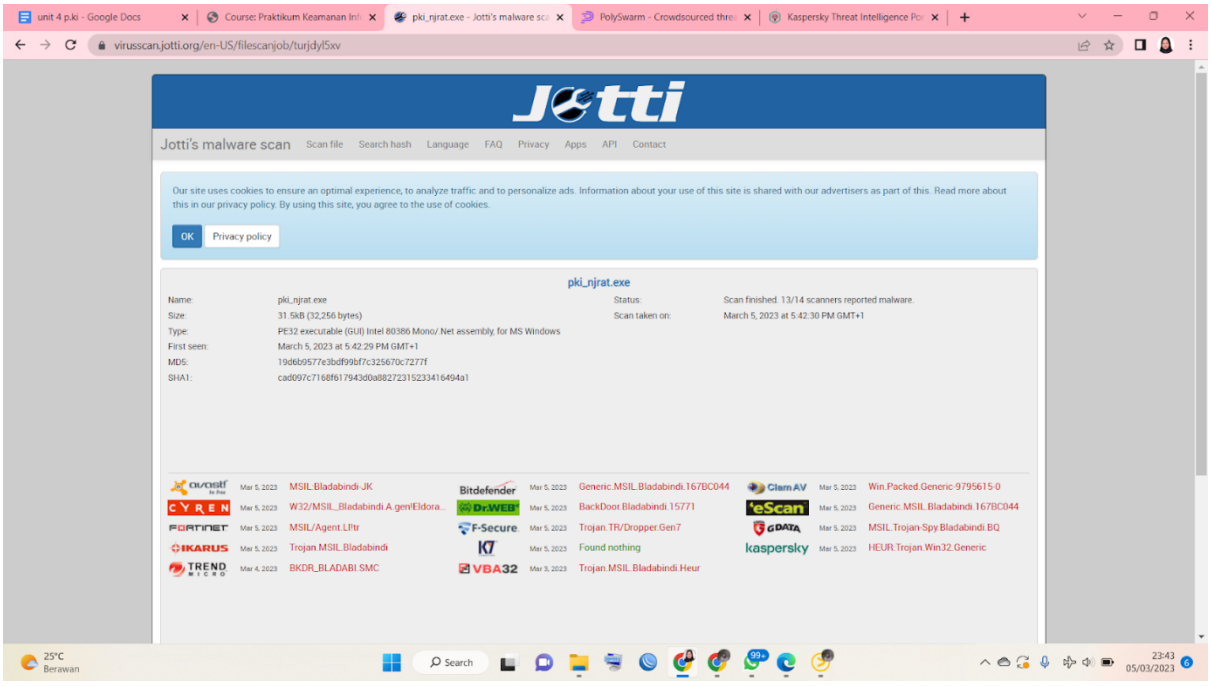


3) VirSCAN


unit 4 p.ki - Google Docs
Course: Praktikum Keamanan Inf
PolySwarm - Crowdsourced threa
Kaspersky Threat Intelligence Po
opentip.kaspersky.com/78369C59EC3DEB46F067FFE040C146332ABFB27C82F9AE849D0A7C5156FA6123/results?tab=upload
Kaspersky Threat Intelligence Portal
Report
Analysis
Requests
Premium Services
About Portal
Language selection
Sign in
Sign in to premium version
Report for hash
78369C59EC3DEB46F067FFE040C146332ABFB27C82F9AE849D0A7C5156FA6123
Submit to reanalyze
Malware
Overview
Hits 0
First seen —
Last seen —
Format exe x32
Size 31.50 KB (32256 B)
Signed by —
Packed by —
MD5 19D6B9577E3BDF99BF7C325670C7277F
SHA-1 CAD097C7168F617943D0A882723152334 16494A1
SHA-256 78369C59EC3DEB46F067FFE040C146332 ABFB27C82F9AE849D0A7C5156FA6123
Categories General
Detection names
5 Mar, 2023 23:24
HEUR:Backdoor.MSIL.Bladabindi.gen
5 Mar, 2023 23:24
HEUR:Trojan.MSIL.Crypt.gen
5 Mar, 2023 20:41
HEUR:Trojan.Win32.Generic
5 Mar, 2023 23:24
25°C Berawan
Search
23:43 05/03/2023
HEUR:Trojan-Spy.MSIL.KeyLogger.gen
Dynamic analysis summary
Last scan performed on 5 Mar, 2023 23:43 with an anti-virus databases updated on 5 Mar, 2023 17:18
Detects
6
Total
Malware 6
Adware and other 0
Suspicious activities
1
Total
High 1
Medium 0
Low 0
Extracted files
1
Total
Malware 1
Adware and other 0
Clean 0
Not categorized 0
Network activities
0
Total
Dangerous 0
Adware and other 0
Good 0
Not categorized 0
https://opentip.kaspersky.com/78369C59EC3DEB46F067FFE040C146332ABFB27C82F9AE849D0A7C5156FA6123/results/suspiciousEvents
23:44 05/03/2023

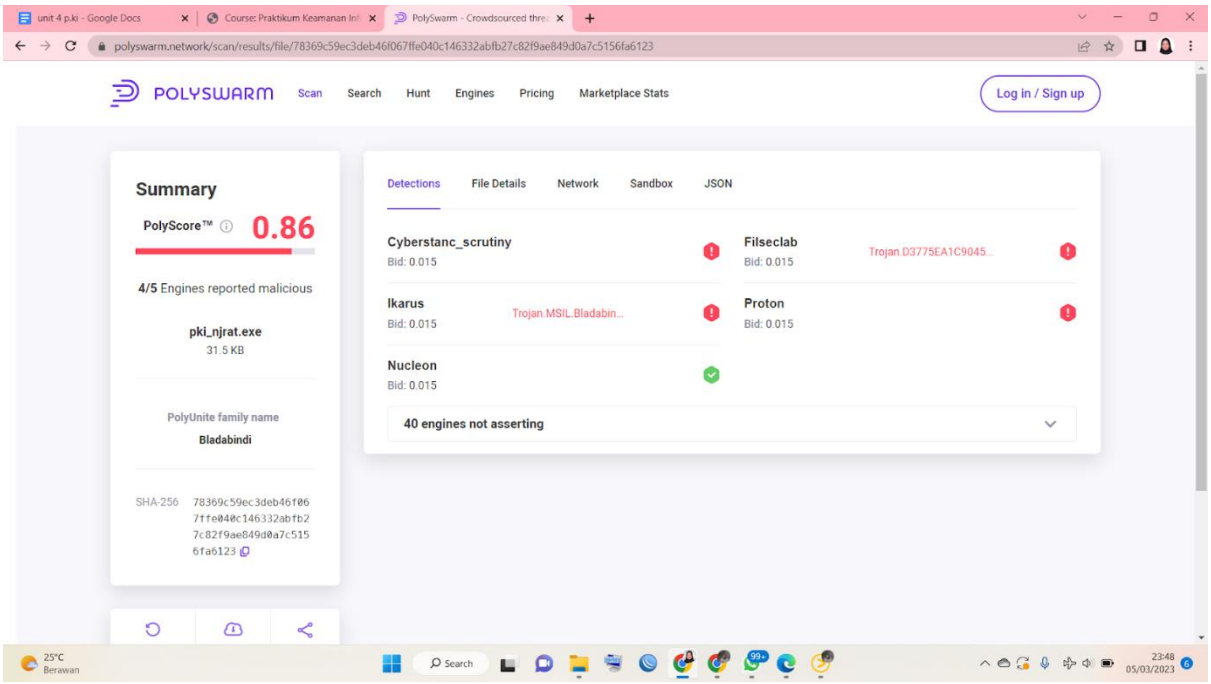


4) Jotti



5) Bitbaan MaLab

6) PolySwarm



Seperti yang ditampilkan pada hasil *scanning malware* dari *file malware* yang telah dibuat menggunakan *software* NJRAT, terdapat beberapa perbedaan hasil dari *scanning* pada setiap *tools* yang digunakan. Di bawah ini merupakan table hasil *scanning* dari beberapa *tools* OSINT tersebut.

No.	OSINT *Tools*	Hasil *Scanning*
1	VirusTotal	59/70
2	OPSWAT (Meta Defender)	10/14
3	VirSCAN	8
4	Jotti	13/14
5	Polyswarm	4/5

Metode OSINT pada *tools* ini pada dasarnya memiliki tujuan yang sama yaitu untuk mengidentifikasi berapa banyak mesin yang dapat mendeteksi *malware* agar terdapat data dari sumber lain yaitu seberbahaya apakah suatu *malware* antara mesin yang satu dengan mesin yang lain. Dapat dilihat pada hasil *scanning* di tabel, bahwa terdapat beberapa perbedaan hasil *scanning malware* dari setiap *tools* yang

digunakan. Ini menandakan bahwa terdapat perbedaan yang efektif dan kuat antar *tools* jika dilihat dari hasilnya.

Dari hasil tersebut juga dapat dilihat bahwa VirSCAN memiliki banyak variasi data atau informasi yang dapat dianalisis, seperti mengenai enkripsi yang terdapat dalam *malware* tersebut. OSINT *tools* lainnya sebenarnya juga memberikan informasi yang serupa, bahkan terdapat informasi yang lebih banyak tentang *file.*

VI. Kesimpulan

1. NJRAT merupakan salah satu *malware* jenis Trojan.
2. OSINT digunakan untuk mengetahui informasi *malware* yang terdapat dalam sebuah aplikasi yang tidak terdapat dalam *tool* OSINT lain.

VII. Daftar Pustaka

Prihadi, Susetyo D. (2016). *Waspada Malware Locky jadi Email Tagihan*. Diakses pada 5 Maret 2023 dari https://www.cnnindonesia.com/teknologi/20160224143955-185-113193/waspada-malware-locky-menyamar-jadi-email-tagihan

Primatyassari, Natasya. (2022). *Kenali Apa Itu Backdoor Attack serta Bagaimana Cara Mencegahnya.* Diakses pada 5 Maret 2023 dari https://www.ekrut.com/media/backdoor

Prayoga, Jordy. (2023). *Apa itu Adware? Kenali Jenis dan Cara Menghindarinya!*. Diakses pada 5 Maret 2023 dari https://gudangssl.id/blog/adware-adalah/

Kuncoro, Arsito. (2022). *Worm Komputer*. Diakses pada 5 Maret 2023 dari http://teknik-informatika-s1.stekom.ac.id/informasi/baca/Worm-Komputer/441b7d76c787c5c38ca3b5f48f1c3aadc82adf18