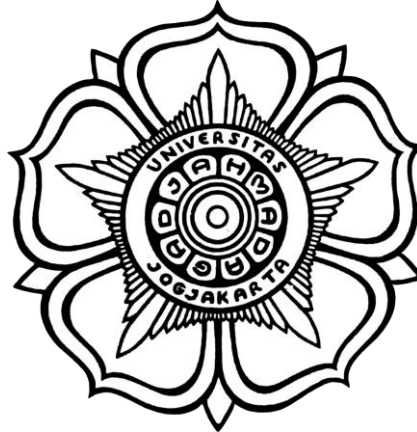


# **LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1**

## **UNIT 4**

### **Analisis Anatomy Malware**



Disusun Oleh :

Nama : Abu Alif Raharjo  
NIM : 21/479770/SV/19537  
Hari, tanggal : Selasa, 28 Februari 2023  
Dosen Pengampu : Anni Karimatul Fauziyyah, S. Kom., M. Eng.

**PROGRAM STUDI DIPLOMA IV TEKNOLOGI REKAYASA INTERNET**

**DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA**

**SEKOLAH VOKASI**

**UNIVERSITAS GADJAH MADA**

**2023**

### **A. Tujuan**

- Meneliti dan menganalisis malware

### **B. 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.

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 tidak menganggapnya sebagai sebuah trojan. [virustotal.com](https://www.virustotal.com) , hanya 4 antivirus yang 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. 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

### **C. Alat dan Bahan**

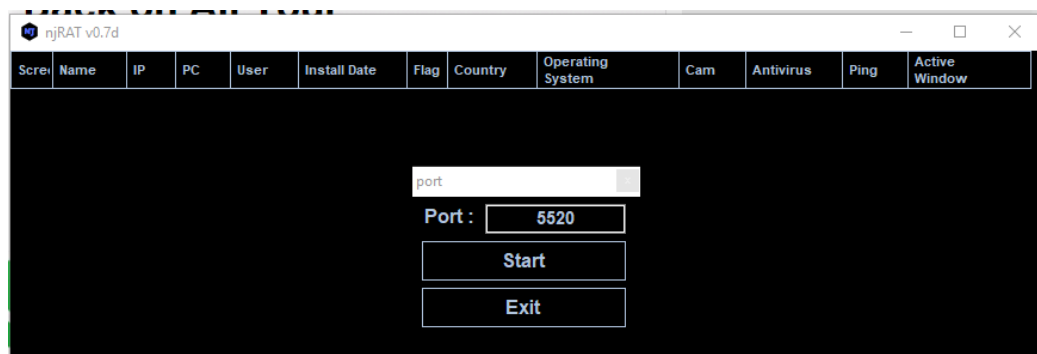
- PC dengan akses internet
- Software njRAT

#### D. 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. 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.
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.

#### 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 5520



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

```

C:\Users\TAJ>ipconfig

Windows IP Configuration

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::d178:240c:fdd9:1862%8
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::e046:5f83:6b1e:676b%4
    IPv4 Address. . . . . : 10.33.107.31
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.33.107.254

```

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

7. Simpan aplikasi hasil build.

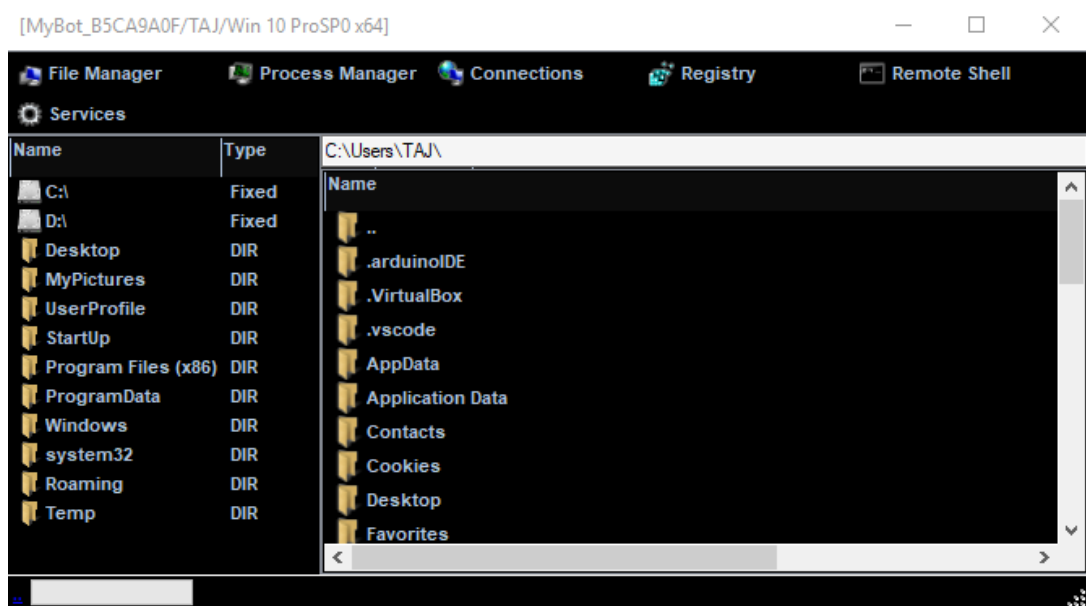
 AbuJadHacker
 28/02/2023 13:09
Application
32 KB

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

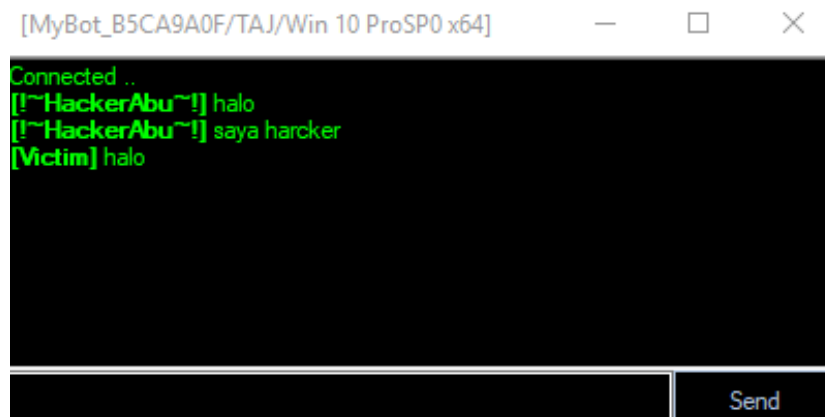
ngRAT v0.7d Port[ 5520 ] Online[ 2 ] Selected[1] REQ[0]

Screen	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam	Antivirus	Ping	Active Window
	MyBot_78DC485B	10.32.167.31	DESKTOP-AIVUJRL	TAJ	23-02-28		N/A	Win 10 Pro SP0 x64	Yes	Windows Defender	980ms	C:\Windows\system32\cmd.exe

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.



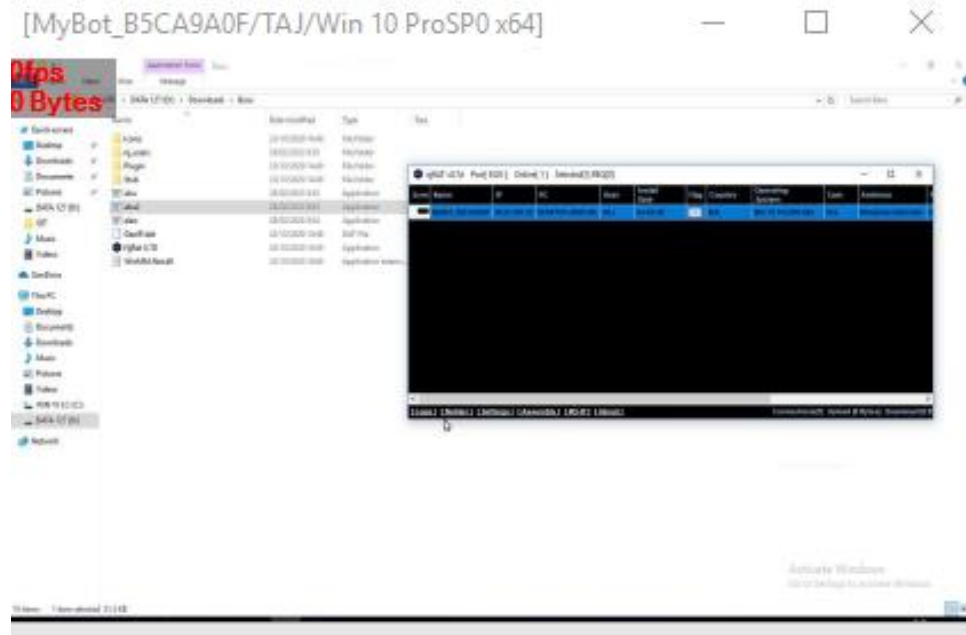
10. Pada menu remote cam maka akan membuka webcam yang ada di komputer victim dan dapat melihat segala aktivitas yang dilakukan oleh victim
11. Pada pilihan chat message , kita dapat mengirimkan pesan ke layar desktop komputer victim, dan user komputer dapat melakukan balasan tanpa bisa menutup chat.



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

AbuladiHacker 28/02/2023 13:09 Application 32 KB

13. Remote Desktop jendela muncul, arahkan kursor mouse ke bagian tengah atas jendela. Panah bawah muncul, klik panah bawah.



## E. Hasil

Hasil scanning dengan metode osint

### 1. VirusTotal

58

70

58 security vendors and no sandboxes flagged this file as malicious

a15ee45066a727084ab83ac18f1dd6117d315f9fdddb6018e1dbfa84265373

AbuladiHacker.exe

peexe assembly

31.50 KB

Size

2023-02-28 02:53:00 UTC

a moment ago

EXE

DETECTION DETAILS BEHAVIOR COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections.

Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	TrojanWin32/Bladabindi.R130484
ALYac	Generic:MSIL/Bladabindi.BAD13174	Anfny-AVL	Trojan[Backdoor]/MSIL/Bladabindi.as
Arcabit	Generic:MSIL/Bladabindi.BADD3376	Avast	MSIL/Bladabindi-JK [Trj]
AVG	MSIL/Bladabindi-JK [Trj]	Avira (no cloud)	TR/Dropper.Gen7
Baidu	MSIL/Backdoor/Bladabindi.a	BitDefender	Generic:MSIL/Bladabindi.BAD13174
BitDefenderTheta	Gen:NN/Zemslf.36276.bmW@ayvEotd	Bkav Pro	W32/HarMinerLL.Trojan
ClamAV	Win.Packed.Generic/9795615-0	CrowdStrike Falcon	Win/malicious_confidence_100% (D)
Cybereason	Malicious.d59ffa	Cylance	Unsafe

## 2. OPSWAT(Meta Defender)

AbuJadHacker.exe

Threat name: Trojan/Njrat!d0myNR7Y

Cast your vote on this file: 0 | 0

The file is not sanitizable

Metascan

Threats detected

12 /16  
ENGINES

Get full report

Upgrade limits

Sandbox Threat Score

No dynamic analysis performed

00 %

View dynamic analysis

Sandbox documentation

Community Insight

User votes

%

View leaderboards

Check out our community

## 3. VirSCAN

Silakan masukkan nilai hash (didukung SHA256, SHA1, MD5)

26/46

AbuJadHacker.exe Ada mesin yang diperiksa

SHA256: A15EE45066A727084A8B9AC18F1DD6117F315F9FEFDD8601F8E1DBFA84265373

SHA1: 5f2a1bf216a5c5355686e78522d955cda9f08b3

MD5: 0807f8bd59ffada3569d8abbfc8dd00b

Ukuran file: 31,5 KB (32256)

Jenis file: Pe

Pengajuan: 2023/02/28 10:00:36 (GMT+7)

Pertama:

Analisis akhir: 2023/02/28 10:01:16 (GMT+7)

Deteksi mesin


Informasi statis

Waktu deteksi terakhir: 2023-02-28 10:01:16

Mendeteksi

mesin	hasil	mesin	hasil
AVG	MSIL:Bladabindi-JK	Authentium	W32/MSIL_Bladabindi.Agent! Eldorado
Antiy	Trojan[Pintu Belakang]/MSIL_Bladabindi.as	Arcabit	Generik.MSIL.Bladabindi.BADD3376
JiangMin	TrojanDropper.Autoit.dce	Avast	MSIL:Bladabindi-JK
Comodo	Backdoor.MSIL.Bladabindi.BA@7oej5x	Emsisoft	IL:Trojan.MSIL.Zilla.7117 (B)
AhnLab	Troya/Win32.Bladabindi.R130484	Meningkat	Backdoor.njRAT11.9E49 (KLASIK)

## 4. Jotti



Jotti's malware scan
Scan file
Search hash
Language
FAQ
Privacy
Apps
API
Contact

Our site uses cookies to ensure an optimal experience, to analyze traffic and to personalize ads. Information about your use of this site is shared with our advertisers as part of this. Read more about this in our privacy policy. By using this site, you agree to the use of cookies.

OK
Privacy policy

AbuJadHacker.exe

Name:

AbuJadHacker.exe

Status:

Scan finished. 13/14 scanners reported malware.

Size:

31.5kB (32.256 bytes)

Scan taken on:

February 28, 2023 at 4:05:23 AM GMT+1

Type:

PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

First seen:















February 28, 2023 at 4:05:22 AM GMT+1

MD5:

0807f8bd59ffade3569d8abbfc8dd00b

SHA1:

5f2a1bf216a5c5355686e78522d955cdf9f08b3

	Feb 28, 2023	MSIL:Bladabindi-JK		Feb 28, 2023	Generic.MSIL.Bladabindi.BAD13174		Feb 27, 2023	Win.Packed.Generic-9795615-0
	Feb 28, 2023	W32/MSIL_Bladabindi.A.gen/Eldora...		Feb 28, 2023	BackDoor.Bladabindi.15771		Feb 28, 2023	Generic.MSIL.Bladabindi.BAD13174
	Feb 28, 2023	MSIL/Agent.LlTr		Feb 27, 2023	Trojan.TR/Dropper.Gen7		Feb 28, 2023	MSIL.Trojan-Spy.Bladabindi.BQ
	Feb 27, 2023	Trojan.MSIL.Bladabindi		Feb 28, 2023	Found nothing		Feb 28, 2023	HEUR:Trojan.Win32.Generic
	Feb 27, 2023	BKDR_BLADABI.SMC		Feb 27, 2023	Trojan.MSIL.Bladabindi.Heur			

## 5. Bitbaan MaLab

Home


Lang ▼ Log



File

URL

12 Antimalware



### Error

لطفا دوباره وارد شوید.

Ok



## 6. PolySwarm

The screenshot displays the PolySwarm web interface. On the left, a 'Summary' panel shows a PolyScore of 0.99, indicating 11/14 engines reported the file as malicious. The file is identified as 'AbuJadHacker.exe' (31.5 KB) with a PolyUnit family name of 'Bladabindi'. The SHA-256 hash is provided. On the right, a 'Detections' table lists various security engines and their results. Most engines flag the file as malicious, with specific threat names like 'Gene.Win.Harmlet.157...', 'Win.Dropper.njRAT', and 'Trojan.D3775EA1C9045...'. A few engines like 'Nucleon' and 'RedDrip APT Scanner - RAS' show a green checkmark, indicating they did not detect the file as malicious. Navigation tabs at the top include Scan, Search, Hunt, Engines, Pricing, and Marketplace Stats. A 'Log in / Sign up' button is in the top right corner. At the bottom of the summary panel are buttons for Rescan, Download, and Share. A 'Nucleon' button is also visible at the bottom of the detections table.

Detections	File Details	Network	Sandbox	JSON	
Alibaba Bid: 0.0037	Gene.Win.Harmlet.157...	!	CrowdStrike Falcon ML Bid: 0.015	win/malicious	!
Cyberstanc_scrutiny Bid: 0.015		!	DrWeb Bid: 0.015	BackDoor.Bladabindi...	!
Electron Bid: 0.015	Win.Dropper.njRAT	!	Filseclab Bid: 0.015	Trojan.D3775EA1C9045...	!
Ikarus Bid: 0.015	Trojan.MSIL.Bladabindi...	!	Proton Bid: 0.015	Win.Dropper.njRAT	!
SecureAge Bid: 0.015	Malicious	!	SentinelOne Static ML Bid: 0.015		!
XVirus Bid: 0.015	Suspicious.NewThreat...	!	Lionic Bid: 0.015		✓
Nucleon Bid: 0.015		✓	RedDrip APT Scanner - RAS		✓

## F. Pembahasan

### Unit 4 no 1 dan 2 analisis struktur malware

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. 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. Penyebaran malware biasanya melalui koneksi internet seperti pengiriman email, download file, themes, plugin dan program yang sudah disusupi malware. Bahkan saat ini malware bisa menyerang server, sehingga website-website yang berada di dalam server tersebut juga rentan terhadap serangan malware. Dampak malware Memperlambat sistem komputer, apabila malware berhasil masuk pada sistem perangkat, kinerja perangkat akan melambat. Dibutuhkan waktu lama untuk menyala serta dalam penggunaannya pun seluruh sistem menjadi sulit merespon. Kerusakan data dan dokumen, akibat lain dari adanya virus yang menyebar pada perangkat ialah kerusakan pada data serta dokumen. Pada beberapa kasus, kerusakan membuat isi dokumen menjadi berantakan. Namun, malware juga dapat menyebabkan sebuah dokumen tidak dapat dibuka.

## Praktikum Malware NjRAT

Pada praktikum kali ini yang membahas tentang malware njRAT. RAT merupakan singkatan dari *Remote Administrator Tools* yang merupakan suatu aplikasi atau tools 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.) dan Shell control (CMD control). Pada fitur-fitur tersebut yang dapat digunakan yang terletak pada menu njRAT. Untuk melakukannya kita harus mengecek IP Address milik host terlebih dahulu pada *Command Prompt*. Setelah itu klik builder dan masukkan ip host dan port yang ingin digunakan serta simpan hasil build. Maka file yang dibuild tadi jika dibuka akan muncul di tampilan njRAT dan kita dapat menggunakan fitur-fitur yang ada seperti remote cam, chat message, run file, manager dan lain-lain.

Sebuah RAT langsung menghubungkan setup sederhana dimana klien (orang yang menyebarkan) akan menghubungkan ke server tunggal atau beberapa server (komputer korban) secara langsung. Server stabil adalah multithreaded, memungkinkan beberapa klien untuk dihubungkan, bersama dengan keandalan meningkat. RAT yang memanfaatkan sambungan terbalik memiliki beberapa keuntungan utama, seperti keluar masuknya koneksi umumnya tidak terlacak dan tidak terdeteksi atau di block oleh Firewall, seperti Router. Karena remote komputer mengkoneksikan ke remote administrator, sehingga pelaku tidak perlu mengetahui IP korban untuk melakukan sambungan. RAT dapat dikatakan legal jika klien (orang yang menyebarkan) menginformasikan bahwa mereka sedang berada di komputer server (komputer korban). Legal RAT memiliki kontrol penuh yang baik. Mereka dapat mengakhiri sambungan setiap saat mereka inginkan dan tidak ada backdoor. RAT dikatakan ilegal jika orang yang berada di komputer server (komputer korban) tidak tahu jika pelaku (orang yang menyebarkan) tersambung dan mereka tidak akan mengetahui sampai pelaku melakukan aksi. Komputer korban tidak mempunyai control untuk kill koneksi dengan pelaku (kecuali mereka memutuskan sambungan internet), tapi ini hanya untuk sementara, karena adanya backdoor yang tertanam pada komputer korban sehingga akan tetap tersambung dengan pelaku jika komputer korban terhubung lagi dengan internet. Terdapat beberapa contoh aplikasi RAT legal seperti TeamViewer, Ammyy Admin, dan Mikogo. Sedangkan untuk yang ilegal yaitu Port Forwarding / Forwarding Port atau juga dikenal sebagai Port Pemetaan. NJRAT 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 dimonitoring / dikendalikan melalui PC host yang berada pada satu jaringan melalui akses IP dan port yang telah ditentukan di awal.

## **G. Kesimpulan**

Kesimpulan pada praktikum kali ini antara lain :

1. njRAT merupakan salah satu malware jenis Trojan yang menginfeksi komputer victim melalui instalasi sebuah program. Ketika malware telah terpasang, maka segala bentuk kegiatan komputer victim akan dapat dimonitor/dikendalikan oleh komputer host yang berada pada satu jaringan melalui akses IP address dan port number yang telah ditentukan sebelumnya.
2. RAT merupakan singkatan dari Remote Administrator Tools yang merupakan suatu aplikasi atau tools 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.), dan Shell control (CMD control).

## **H. Daftar Pustaka**

Choiri, E. O. (2021, September 8). *Apa Itu Malware? Bahaya dan Cara Mengatasinya*. Gudangssl. [https://gudangssl.id/blog/apa-itu-](https://gudangssl.id/blog/apa-itu-malware/#:~:text=Penyebaran%20malware%20biasanya%20melalui%20koneksi)

[malware/#:~:text=Penyebaran%20malware%20biasanya%20melalui%20koneksi](https://gudangssl.id/blog/apa-itu-malware/#:~:text=Penyebaran%20malware%20biasanya%20melalui%20koneksi)

*Pengertian Malware serta Jenis dan Cara Mengatasinya Dengan Tepat*. (n.d.).

[Www.cloudmatika.co.id](https://www.cloudmatika.co.id). Retrieved March 5, 2023, from <https://www.cloudmatika.co.id/blog-detail/apa-itu-malware>

publisher. (2022, December 20). *Holiday Season Sees Onslaught of Ransomware,*

*DDoS Attacks*. TechNewsWorld. <https://www.technewsworld.com/story/holiday-season-sees-onslaught-of-ransomware-ddos-attacks-177544.html>