

LAPORAN PRAKTIKUM
KEAMANAN INFORMASI 1

PERTEMUAN 3

Analisis Anatomy Malware



DISUSUN OLEH

Nama : Muhamad Alan Dharma Saputro S
NIM : 21/481348/SV/19761
Hari, Tanggal : Selasa, 28 Februari 2023
Dosen Pengampu : Anni Karimatul Fauziyyah, S.Kom., M.Eng.
Kelas : RI4AA

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
YOGYAKARTA
2022

A. Tujuan

1. 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.

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 diawal.

C. Alat dan Bahan

1. PC dengan akses internet

D. Intruksi 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.

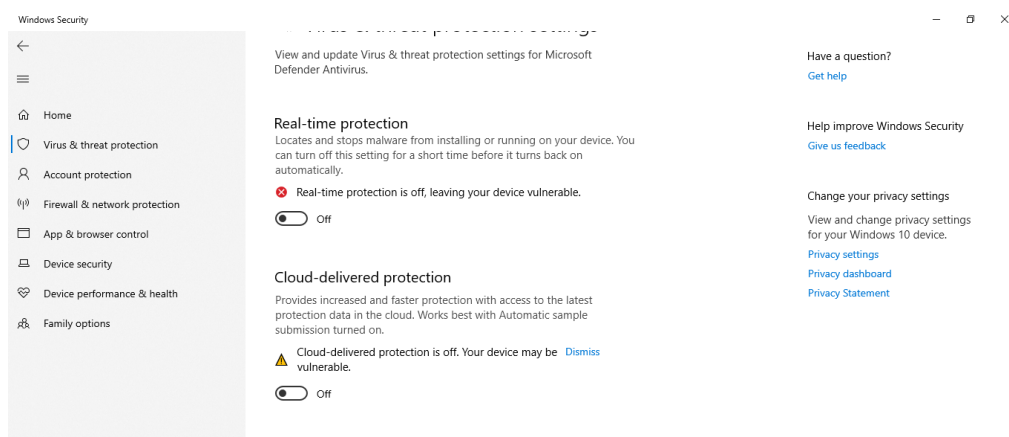
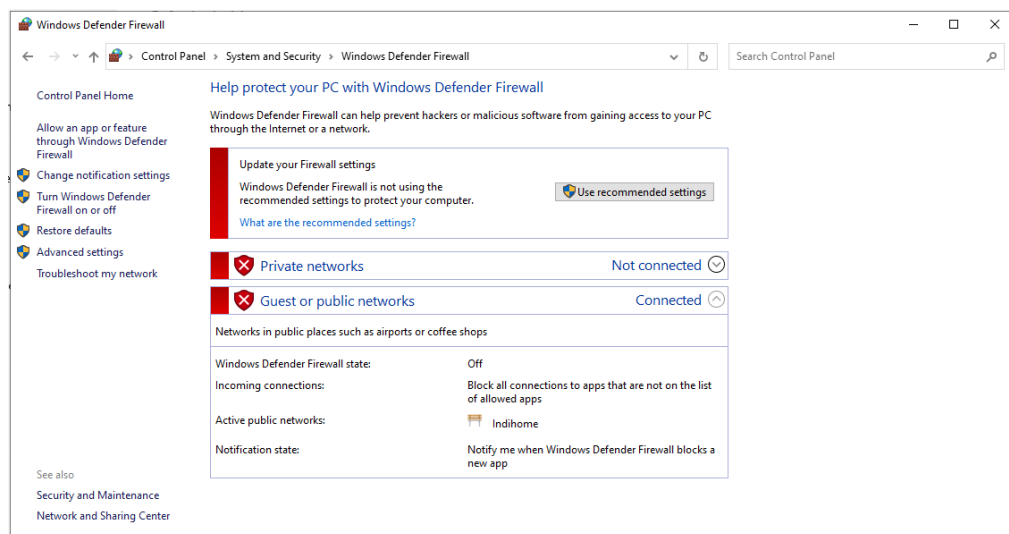
Contoh jenis malware antara lain: Ransomware, Trojan, Hoax, Adware, Malware, PUP, Exploit, Exploit Kit dan Kerentanan. Cari malware dengan mengunjungi situs web berikut menggunakan istilah pencarian berikut:

- Dasbor Lanskap Ancaman Pusat Ancaman McAfee
- Pusat Ancaman MalwarebytesLabs (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

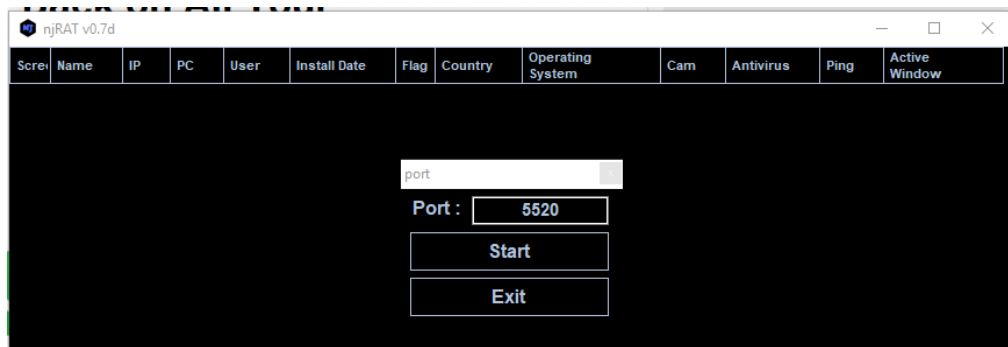
1. Jalankan virtual machine windows
2. Clone VM windows, untuk dijadikan target
3. Pada VM windows yang dijadikan host matikan semua antivirus dan firewall pada kedua komputer yang digunakan untuk memakai aplikasi njrat ini.



4. Download dan ekstrak aplikasi NJRAT kemudian run aplikasi NJRAT pada komputer host. Dapat menggunakan link dibawah atau file pada eLok.

<https://github.com/adarift/njRAT/releases/tag/v0.7D>

Masukkan port yang ingin digunakan **5520**



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

```

C:\> Command Prompt

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::a484:aedb:bd1:bb77%7
    IPv4 Address. . . . . : 192.168.137.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 12:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 13:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

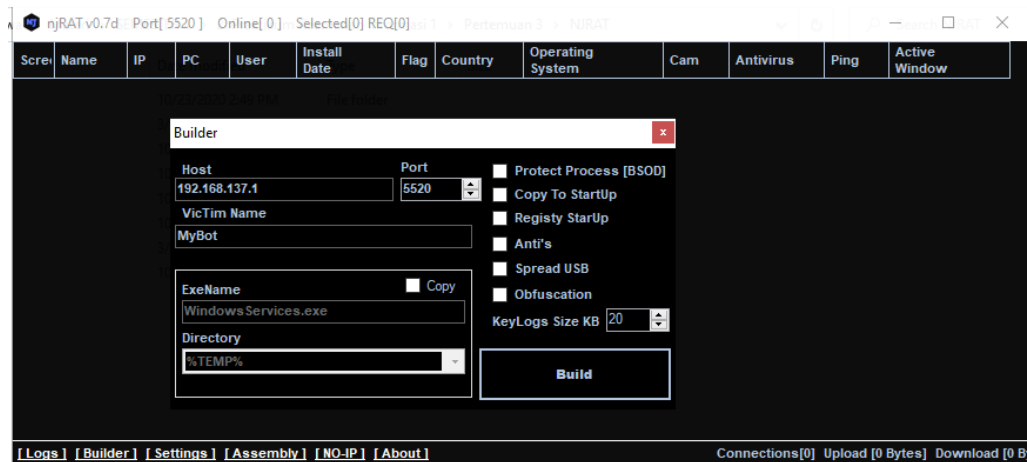
Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2001:448a:4045:425f:d09d:11fa:f0b9:90fe
    Temporary IPv6 Address. . . . . : 2001:448a:4045:425f:b1fa:e552:8be9:fa29
    Link-local IPv6 Address . . . . . : fe80::7e74:d334:5695:9645%2
    IPv4 Address. . . . . : 192.168.1.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::1%2
                                192.168.1.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
  
```

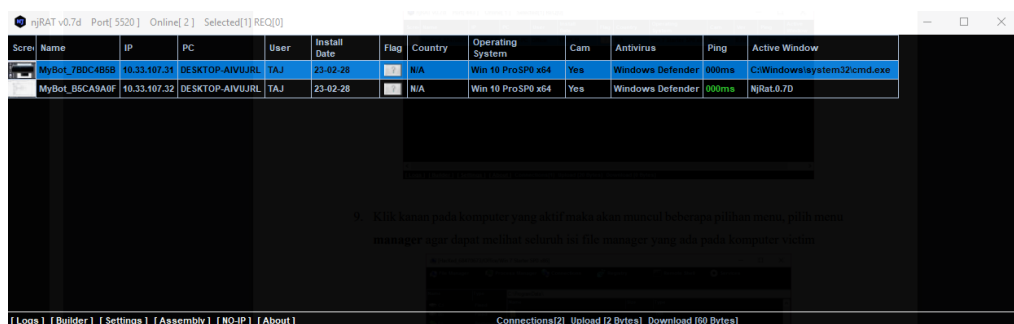
6. Buat aplikasi yang akan dipasang pada komputer victim. Masukkan IP Address host pada kolom host dan port yang sesuai dengan yang kita tentukan tadi pada awal membuka aplikasi NJRAT agar dapat diakses oleh komputer nanti, kemudian klik tombol build.



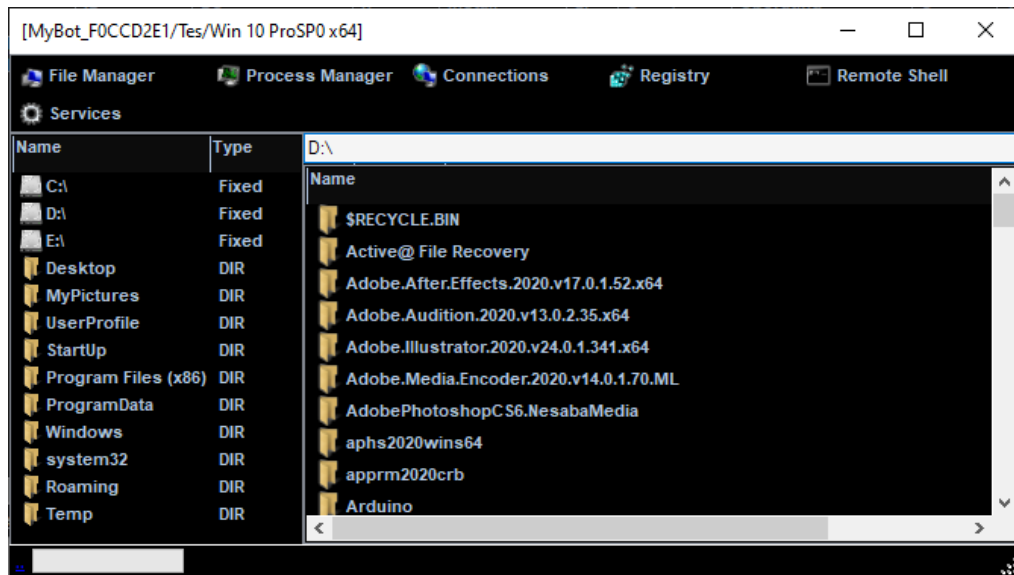
7. Simpan aplikasi hasil build

Name	Date modified	Type	Size
Icons	10/23/2020 2:49 PM	File folder	
nj_users	3/6/2023 2:51 AM	File folder	
Plugin	10/23/2020 2:49 PM	File folder	
Stub	10/23/2020 2:49 PM	File folder	
Alan	3/6/2023 2:59 AM	Application	32 KB
GeolP.dat	10/23/2020 2:49 PM	DAT File	1,137 KB
NjRat 0.7D	10/23/2020 2:49 PM	Application	8,745 KB
NjRat.0.7D	3/6/2023 2:49 AM	WinRAR ZIP archive	9,423 KB
WinMM.Net.dll	10/23/2020 2:49 PM	Application exten...	43 KB

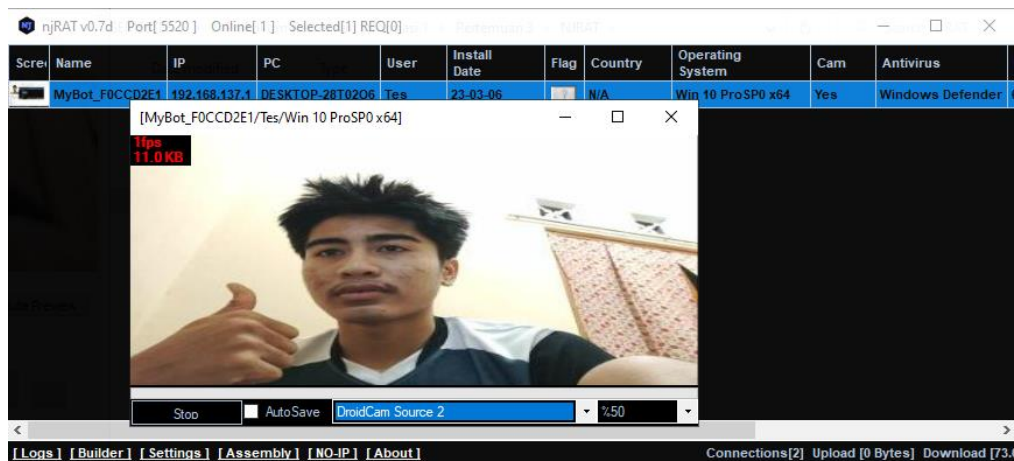
- Kemudian, copykan aplikasi <nama aplikasi> yang sudah telah kita buat ke dalam komputer victim. Kemudian, pada komputer victim jalankan aplikasi tersebut. Ketika sudah terpasang pada komputr victim, NJRAT pada host akan mendeteksi komputer victim



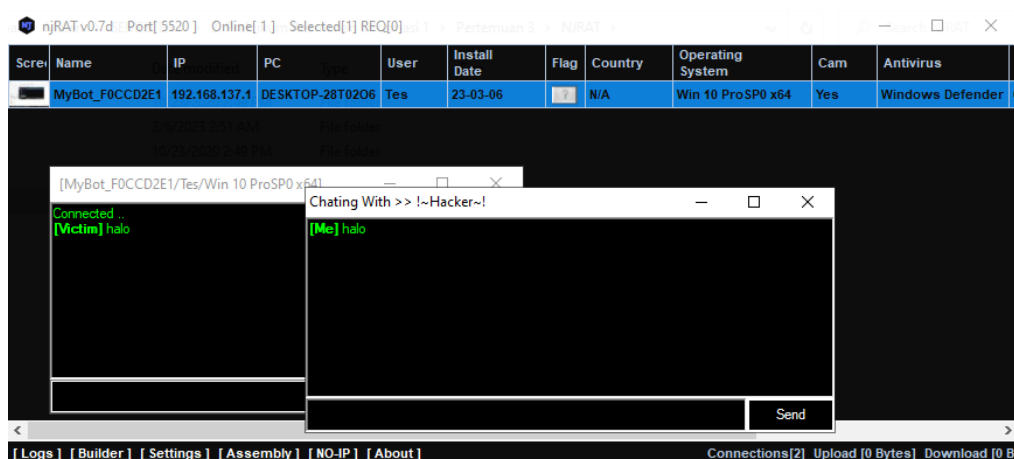
- Klik kanan pada komputer aktif maka akan muncul beberapa pilihan menu, pilih **menu manager** agar dapat melihat seluruh isi file manager yang ada pada komputer victim



10. Pada menu **remote cam** 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

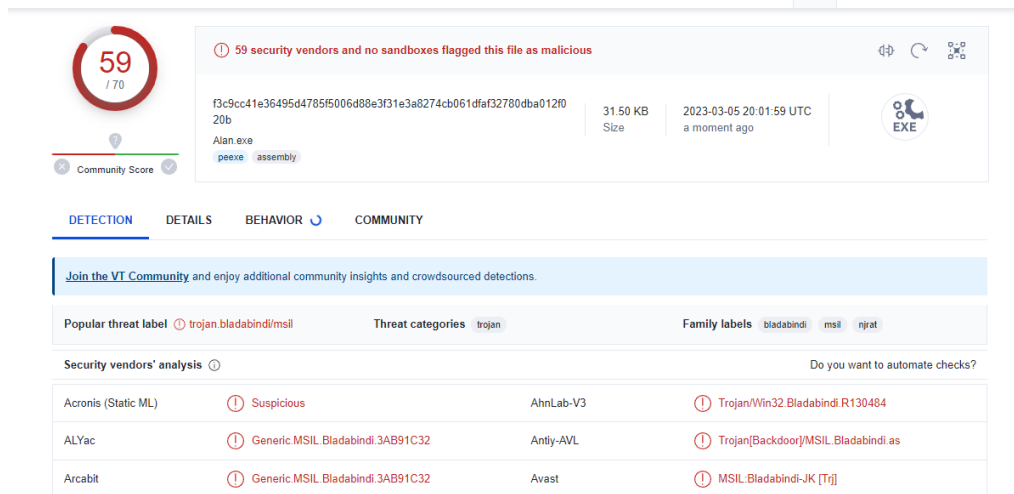


12. File aplikasi dari komputer victim dapat diremot sesuai keinginan.

E. Hasil Praktikum

Hasil scanning dengan metode osint

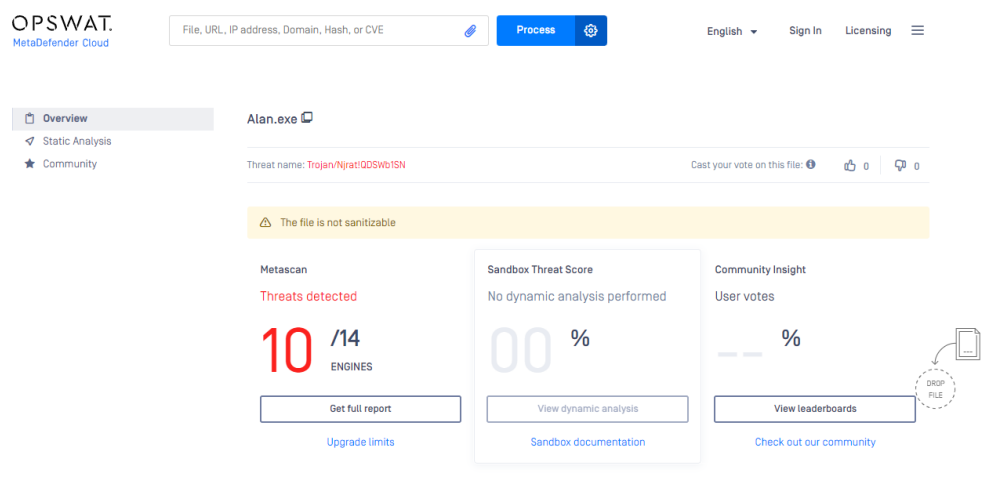
1. VirusTotal



The screenshot shows the VirusTotal interface for a file named 'Alan.exe'. The file has a SHA256 hash of f3c9cc41e36495d4785f5006d88e3f31e3a8274cb061dfa32780dba012f020b, a size of 31.50 KB, and was uploaded on 2023-03-05 20:01:59 UTC. The file is flagged as malicious by 59 security vendors. The detection tab shows a popular threat label of 'trojan.bladabindi/msil' and threat categories of 'trojan'. The security vendors' analysis table shows the following results:

Security vendor	Analysis
Acronis (Static ML)	Suspicious
AhnLab-V3	Trojan/Win32.Bladabindi.R130484
ALYac	Generic.MSIL.Bladabindi.3AB91C32
Antiy-AVL	Trojan[Backdoor]/MSIL.Bladabindi.as
Arcabit	Generic.MSIL.Bladabindi.3AB91C32
Avast	MSIL:Bladabindi-JK [Trj]

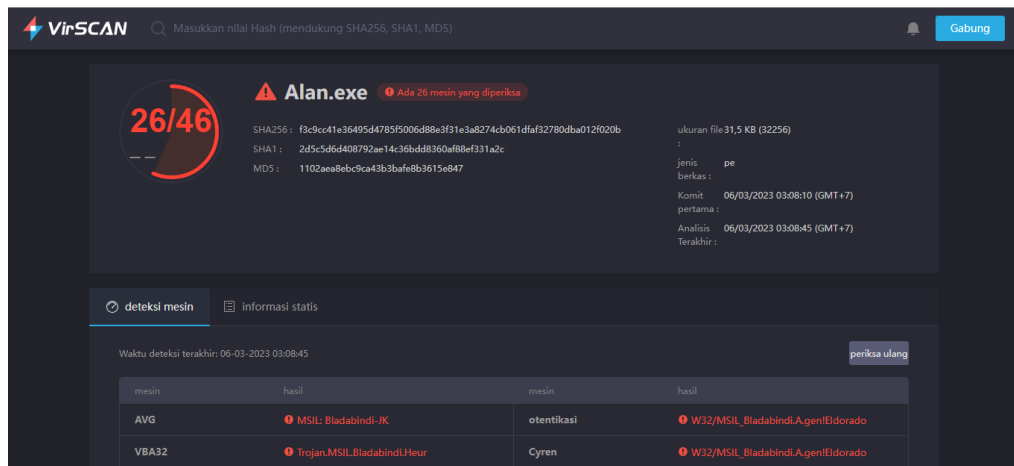
2. OPSWAT (Meta Defender)



The screenshot shows the OPSWAT interface for a file named 'Alan.exe'. The file is not sanitizable. The Metascan section shows 10 threats detected out of 14 engines. The Sandbox Threat Score is 00%. The Community Insight section shows user votes. The file is flagged as malicious by 10 engines. The detection tab shows the following results:

Engine	Result
Metascan	10 / 14

3. VirSCAN



The screenshot shows the VirSCAN interface for a file named 'Alan.exe'. The file has a SHA256 hash of f3c9cc41e36495d4785f5006d88e3f31e3a8274cb061dfa32780dba012f020b, a size of 31.5 KB (32256 bytes), and was uploaded on 06/03/2023 03:08:10 (GMT+7). The file is flagged as malicious by 26/46 engines. The detection tab shows the following results:

mesin	hasil	mesin	hasil
AVG	MSIL:Bladabindi-JK	otentikasi	W32/MSIL_Bladabindi.AgeniEldorado
VBA32	Trojan.MSIL.Bladabindi.Heur	Cyren	W32/MSIL_Bladabindi.AgeniEldorado

4. Jotti

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.

OKPrivacy policy

Alan.exe

Name:Alan.exe

Status:Scan finished. 13/14 scanners reported malware.

Size:31.5kB (32,256 bytes)

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

First seen:March 5, 2023 at 9:14:36 PM GMT+1

MD5:1102aee8ebc9ca43b3baf8b3615e847

SHA1:2d5c5d6d408792ae14c36bdd8360af88ef331a2c

Bitdefender

Generic.MSIL.Bladabindi.3AB91C32

ClamAV

Win.Packed.Generic-9795615-0

Cyren

W32/MSIL.Bladabindi.A.gen/Eldora...

DrWeb

BackDoor.Bladabindi.15771

eScan

Generic.MSIL.Bladabindi.3AB91C32

F-Secure

Trojan.TRI/AD.Bladabindi.HQ

gDATA

MSIL.Trojan-Spy.Bladabindi.BQ

Ikarus

Trojan.MSIL.Bladabindi

K7

Found nothing

kaspersky

HEUR:Trojan.Win32.Generic

Quat

MSIL.Bladabindi-JK

Trend Micro

BNDR.BLADABI.SMC

VBA32

Trojan.MSIL.Bladabindi.Heur

5. Bitbaan MaLab

BitBaan MALab

FileURL

12 Antimalware

✖

Error

لطفا دوباره وارد شوید.

Ok

6. PolySwarm

POLYSWARM

Scan

Search

Hunt

Engines

Pricing

Marketplace Stats

Log in / Sign up

Summary

PolyScore™

0.99

15/18 Engines reported malicious

Alan.exe

31.5 KB

PolyUnit family name

Bladabindi

SHA-256

f3c9cc41e36495d4785f5006d88e3f31c3a827

Detections

File Details

Network

Sandbox

JSON

Alibaba

Bid: 0.0037

Gene.Win.Hamlet.157...

ClamAV

Bid: 0.015

Win.Packed.Generic-9...

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.4F3FC3D23A8DC...

Ikarus

Bid: 0.015

Trojan.MSIL.Bladabin...

NanoAV

Bid: 0.015

Trojan.Win32.Gen8.ec...

Proton

Bid: 0.015

Win.Dropper.njRAT

F. Pembahasan

Analisis Struktur Malware

Jenis Malware antara lain :

1. Virus

Virus memiliki cara kerja yang akan menduplikasi dirinya tanpa sepengetahuan. Virus memodifikasi program komputer dan memasukkan serangkaian kode. Virus komputer memiliki tujuan untuk menginfeksi dan merusak sistem yang mengakibatkan data atau aplikasi tersebut tidak bisa diakses atau bahkan hilang.

2. Worm

Worm merupakan malware yang memiliki cara kerja yang sama seperti virus namun memiliki tujuan berbeda dengan virus. 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 bandwidth jaringan.

3. Trojan

Malware Trojan akan menyamar menjadi program yang sah atau valid untuk mengelabui pengguna. Trojan akan terus bersembunyi di komputer sampai pengguna membuka program tersebut. Trojan juga bisa menular ke perangkat yang lain melalui WiFi ketika ada salah satu device yang terinfeksi.

4. Ransomware

Serangan malware yang dikirim peretas untuk mengunci dan mengenkripsi perangkat komputer milik korban. Ransomware akan menolak akses ke data atau sistem komputer sampai pengguna membayar uang tebusan.

Pada praktikum ini menggunakan malware Trojan, sehingga saya akan membahas tentang Trojan. Trojan merupakan malware yang dapat menyamar baik menjadi file, software, link, bahkan email yang seolah-olah malware tersebut merupakan file yang aman. Selain menyamar sebagai program, sebuah komputer juga bisa terjankit Trojan horse lewat social engineering atau rekayasa sosial. Fortinet menuliskan bahwa taktik ini dijalankan para penjahat siber untuk memaksa pengguna mengunduh file berbahaya yang kerap disembunyikan di iklan pop-up ataupun tautan situs web. Malware Trojan ini memiliki format “.exe” namun malware ini tidak dapat bergerak sendiri, ia dikendalikan oleh hacker yang mengirimnya.

Cara kerja Trojan cukup sederhana, yang mana malah membuat banyak orang terjebak pada malware ini.

1. Hacker mengirimkan pancingan kepada target. Pancingan yang digunakan tergantung kondisi, malware dapat menyamar menjadi file, software, atau link.
2. Jika target terpancing, target akan membuka file malware Trojan yang mereka terima.
3. Saat Trojan aktif, malware akan mengirimkan seluruh info yang diinginkan hacker.
4. Hacker dapat mengendalikan sistem dan melakukan tindak kejahatan.
5. Perangkat dan server yang terinfeksi dapat menularkan Trojan ke perangkat atau website lain yang saling terhubung.

Jika perangkat saling terhubung baik melalui server maupun secara langsung malware Trojan dapat menginfeksi perangkat tersebut tanpa sepengetahuan pengguna. Dampaknya informasi yang terdapat pada perangkat ataupun server dapat dicuri oleh hacker yang menyebarkan malware ini. Sistem dapat dirusak, data dapat dihancurkan atau dihapus, komputer dapat diambil alih.

Praktikum Malware NJRAT

njRAT (Remote Access Trojan) memiliki kemampuan untuk mencatat penekanan tombol, mengakses kamera, mencuri informasi data, mengunggah atau mengunduh file melalui perangkat lunak server Command & Control (CnC), penyerang memiliki kemampuan untuk membuat dan mengkonfigurasi malware untuk menyebar melalui drive USB atau sharing file. Malware Njrat dijalankan secara manual oleh pelaku untuk mengambil alih akses komputer target. Namun perlu diperhatikan jika komputer target mengaktifkan firewall file tidak akan berjalan atau tidak dapat digunakan.

Maka pada praktikum ini matikan terlebih dahulu semua firewall dan antivirus pada komputer agar dapat memulai praktikum. Langkah pertama untuk memulai praktikum yaitu install software Njrat melalui link yang sudah disediakan. Masuk pada software Njrat lalu diminta untuk memasukkan port, tuliskan 5520 sesuai modul (tidak diharuskan menggunakan 5520). Lalu masuk pada cmd ketikkan “ipconfig” untuk melihat IP Address yang digunakan komputer. Kembali ke Njrat, klik builder pada bagian kiri bawah untuk membuat file “.exe” dengan memasukkan IP Address komputer dan port yang digunakan. lalu simpan file tersebut.

File tersebut yang digunakan untuk memberikan seluruh informasi dari komputer yang digunakan. Minta file pada komputer target agar komputer target dapat dihack. Buka file dari komputer target sehingga dapat diambil alih. Pada software Njrat terdapat beberapa tool untuk mendapatkan informasi dari komputer target yaitu dapat melihat file manager dari target dan aktivitas dari target menggunakan kamera. Tidak hanya itu pelaku dapat mengirimkan pesan pada target yang mana pesan tersebut tidak dapat dimatikan oleh target, hanya pelaku yang dapat mematikan tool pesan tersebut.

Penyebaran malware tersebut menggunakan teknik social engineering yaitu teknik yang menggunakan kelemahan manusia, sehingga user tanpa curiga langsung mengeksekusi sebuah program yang dianggapnya baik-baik saja. Virus komputer dibuat dengan tujuan yang tidak baik yaitu untuk pencurian data pada komputer tanpa sepengetahuan dari pemiliknya. Banyak efek negatif yang ditimbulkan oleh virus komputer diantaranya rusaknya data dan program pada komputer sehingga data tersebut tidak dapat dibuka, ataupun program yang ada pada komputer tidak dapat berjalan.

Analisis Malware Dengan Metode OSINT

Pada setiap scanner, dari file yang dideteksi file tersebut merupakan kategori malware Trojan. Sesuai dengan pembahasan sebelumnya njRAT merupakan Remote Access Trojan sehingga file tersebut sudah semestinya file Trojan. Pada hasil scanning file Trojan terdapat beberapa Trojan seperti Fileclab, NanoAV, DrWeb, Jiangmin dan lain-lain. Kebanyakan dari file Trojan tersebut berupa Trojan backdoor dan Trojan ransomware. Dari 14 ancaman yang ada pada file Trojan tersebut, dapat terdeteksi 10 ancaman yang merupakan malware dan file jahat.

Terdapat beberapa tindakan yang dapat dilakukan saat komputer sudah terkena malware khususnya Trojan antara lain yaitu :

1. Menghapus Trojan

Jika Trojan terdeteksi di sistem komputer, tindakan pertama yang perlu dilakukan adalah menghapus Trojan tersebut. Bisa dilakukan dengan menggunakan program antivirus terbaru dan melakukan pemindaian penuh pada sistem.

2. Memulihkan file yang terinfeksi

Jika Trojan telah merusak atau mengenkripsi file pada sistem komputer, upaya perbaikan atau pemulihan file tersebut perlu dilakukan. Hal ini dapat meliputi penggunaan program khusus atau layanan pemulihan data profesional.

3. Mengubah kata sandi

Beberapa jenis Trojan, seperti Trojan banking, dapat mencuri informasi login dan kata sandi pengguna. Oleh karena itu, jika Trojan telah terdeteksi pada sistem komputer, sebaiknya segera mengubah kata sandi untuk akun yang mungkin terpengaruh.

4. Memperbarui perangkat lunak dan sistem operasi

Trojan dapat memanfaatkan kelemahan dalam sistem operasi atau perangkat lunak untuk masuk ke dalam sistem komputer. Oleh karena itu, pastikan selalu memperbarui perangkat lunak dan sistem operasi dengan patch keamanan terbaru.

5. Backup data

Untuk menghindari kehilangan data karena Trojan atau serangan malware lainnya, pastikan selalu membackup data secara teratur dan menyimpannya di tempat yang aman.

6. Hindari sumber yang tidak terpercaya

Untuk mencegah infeksi Trojan dan malware lainnya, hindari mengunduh program atau file dari sumber yang tidak diketahui atau tidak terpercaya.

7. Konsultasi dengan ahli keamanan komputer

Jika tidak yakin bagaimana melakukan tindakan yang diperlukan atau jika Trojan sangat sulit untuk dihapus, sebaiknya konsultasi dengan ahli keamanan komputer yang terpercaya.

G. Kesimpulan

Kesimpulan yang didapatkan dari praktikum kali ini yaitu:

1. Malware Trojan akan menyamar menjadi program yang sah atau valid untuk mengelabui pengguna. Trojan akan terus bersembunyi di komputer sampai pengguna membuka program tersebut.
2. Dampak yang ditimbulkan jika di komputer terdapat file Trojan informasi yang terdapat pada perangkat ataupun server dapat dicuri oleh hacker yang menyebabkan malware ini. Sistem dapat dirusak, data dapat dihancurkan atau dihapus, komputer dapat di ambil alih.

3. njRAT (Remote Access Trojan) memiliki kemampuan untuk mencatat penekanan tombol, mengakses kamera, mencuri informasi data, mengunggah atau mengunduh file melalui perangkat lunak server Command & Control (CnC), penyerang memiliki kemampuan untuk membuat dan mengkonfigurasi malware untuk menyebar melalui drive USB atau sharing file.
4. Pada hasil scanning file Trojan terdapat beberapa Trojan seperti Fileclab, NanoAV, DrWeb, Jiangmin dan lain-lain. Kebanyakan dari file Trojan tersebut berupa Trojan backdoor dan Trojan ransomware.

H. Daftar Pustaka

- 10 Jenis-Jenis malware Yang Dapat Mengancam Data Perusahaan Anda. 10 Jenis-Jenis Malware yang Harus Anda Waspadai. (2022, December 24). Retrieved March 6, 2023, from <https://www.cloudmatika.co.id/blog-detail/jenis-jenis-malware>
- Benefita. (2021, July 7). Ketahui Cara Kerja trojan Dan Cara Mengatasinya. Niagahoster Blog. Retrieved March 6, 2023, from <https://www.niagahoster.co.id/blog/cara-kerja-trojan/>
- Stratton, A. (2022, October 9). NJRAT malware analysis. Medium. Retrieved March 6, 2023, from <https://infosecwriteups.com/njrat-malware-analysis-8e90dce07a9e>
- Widiyasono, N. (2016, December). (PDF) Investigasi Serangan malware Njrat Pada PC - ResearchGate. Jurnal Edukasi dan Penelitian Informatika (JEPIN) 2. Retrieved March 6, 2023, from https://www.researchgate.net/publication/318962355_Investigasi_Serangan_Malware_Njrat_Pada_PC