

LAPORAN PRAKTIKUM
KEAMANAN INFORMASI 1 (SVRI214404)

Unit 3, Analisis *Malware*



DISUSUN OLEH:

Nama : Reyhan Gusnur Putra

NIM : 21/477927/SV/19223

Hari, Tanggal : Selasa, 28 Februari 2023

Kelas : A

PROGRAM STUDI TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA

2023

A. Tujuan

- Meneliti dan menganalisis struktur malware
- Mampu mengembangkan malware trojan dengan Njrat
- Mampu analisis malware dengan metode osint

B. Dasar Teori

Malware adalah perangkat lunak yang dibuat dengan tujuan memasuki dan terkadang merusak sistem komputer, jaringan, atau server tanpa diketahui oleh pemiliknya. Istilah malware diambil dari gabungan potongan dua kata yaitu malicious “berniat jahat” dan software “perangkat lunak”. Tujuannya untuk merusak atau mencuri data dari perangkat yang dimasuki. Malware biasanya disusupkan ke dalam jaringan internet. Jika secara manual memasukkan ke dalam komputer korban tentu saja sangat sulit. Jadi kebanyakan peretas melakukan aksinya menggunakan bantuan jaringan internet.

Trojan adalah malware yang memasuki sistem dengan cara menyamar sebagai file lain yang seolah aman, kemudian merusak sistem di dalamnya. Hal ini yang membuat trojan berbahaya karena sulit dikenali. Kamu bisa saja tidak sengaja mengunduh trojan yang dikemas dalam bentuk software atau tautan berbahaya.

Trojan juga dikenal dengan nama Trojan Horse. Istilah ini muncul bukan tanpa alasan, sebetulnya ada peristiwa sejarah dibalik nama ini. Istilah Trojan Horse mengadaptasi dari cerita Yunani kuno, yaitu masa Perang Troya.

OSINT berasal dari dua istilah yakni “Open Source” dan “Intelligence”. “Open Source” mengacu pada informasi apapun yang diperoleh dari internet secara online. Sedangkan yang dimaksud “Intelligence” adalah informasi yang sudah dikumpulkan untuk tujuan profesional. Sehingga dapat kita definisikan OSINT sebagai informasi apa pun yang dapat dikumpulkan secara legal dari sumber publik yang terbuka secara bebas tentang individu atau organisasi. Dalam praktiknya, OSINT tidak hanya informasi yang didapatkan dari internet, tetapi bisa juga berupa informasi berupa teks seperti surat kabar, gambar, video, webinar, dan bahkan pidato publik semuanya termasuk dalam istilah tersebut.

C. Alat dan Bahan

1. PC atau laptop
2. Jaringan internet
3. Software Njrat

D. Tugas dan hasil

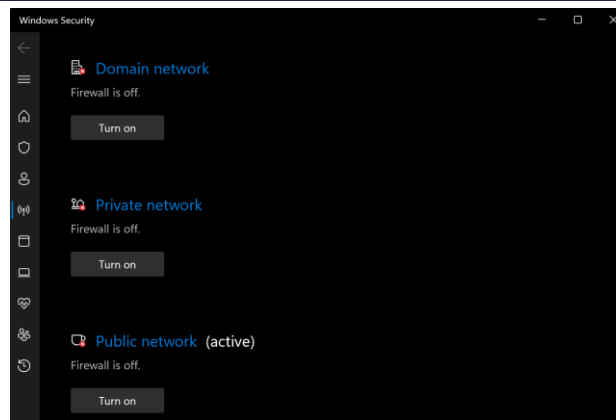
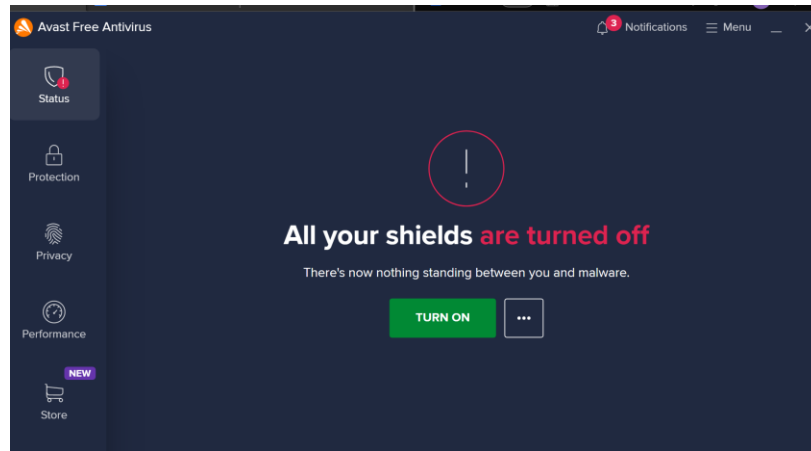
1. Kerjakan modul praktikum unit 4 no 1 dan 2 analisis struktur malware
 - a. Menggunakan mesin pencari favorit Anda, lakukan pencarian untuk malware terbaru. Selama pencarian Anda, pilih empat contoh malware, masing-masing dari jenis malware yang berbeda, dan bersiaplah untuk membahas detail tentang apa yang dilakukan masing-masing, bagaimana masing-masing ditransmisikan, dan dampak masing-masing penyebabnya.
 - Ransomware artinya program tebusan, yaitu sebuah program jahat (malicious software) yang dapat mengunci, menghapus, dan mengambil data tertentu dari perangkat target. Setelah ransomware masuk ke dalam perangkat Anda, program tersebut akan mengunci file, program, atau data digital lainnya. Ini mengakibatkan Anda tidak dapat mengakses atau menggunakan data tersebut. Selanjutnya, pelaku cybercrime tersebut dapat meminta tebusan jika Anda ingin mendapatkan password untuk membuka file tersebut.
 - Virus trojan adalah sebuah malware yang sering menyamar sebagai file, email, bahkan link yang seolah-olah berasal dari lembaga resmi. Trojan adalah malware yang dapat membuat para peretas memiliki akses bebas ke dalam device Anda. Mereka bisa mencuri dan mengacaukan sistem yang ada pada perangkat tersebut.
 - Exploit kit adalah seperangkat program yang digunakan penyerang untuk melakukan serangan terhadap kerentanan yang telah diketahui dalam perangkat lunak/software. Cara kerja exploit kit adalah dengan memanfaatkan kerentanan keamanan korban ketika korban sedang menjelajahi internet.
 - PUP adalah singkatan dari Potentially Unwanted Program, dalam artian adalah program yang terunduh meskipun tidak diinginkan oleh pengguna tersebut, contohnya seperti Adware ataupun Spyware. Biasanya PUP ini akan menumpang/disisipkan pada aplikasi/software gratis yang diinstal oleh pengguna, aplikasi/software ini biasa disebut Freeware. Bagaimanapun juga PUP tidak bisa dikatakan ilegal, karena pengguna sendiri yang memberikan izin akses untuk aplikasi/software tersebut. Meskipun dikatakan demikian, keberadaan PUP sangatlah mengganggu penggunanya. Umumnya PUP

menampilkan iklan pop up dan pada setiap website yang dikunjungi akan selalu muncul iklan.

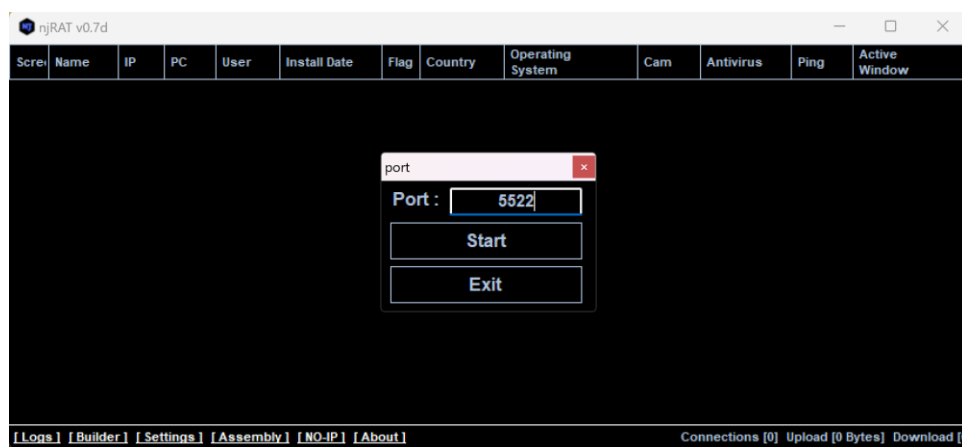
- b. Baca informasi tentang malware yang ditemukan dari pencarian Anda di langkah sebelumnya, pilih salah satu dan tulis ringkasan singkat yang menjelaskan apa yang dilakukan malware, cara penularannya, dan dampaknya.
 - Malware merupakan perangkat lunak yang bekerja dengan memasuki komputer tanpa perizinan 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. Lebih buruk, malware dapat melakukan pencurian data dan informasi yang tersimpan dalam komputer serta menjadi pintu belakang masuknya hacker. 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. Malware tidak diciptakan oleh sembarang orang. Perangkat lunak ini diciptakan oleh para hacker yang memiliki pemahaman tinggi akan perangkat lunak dengan tujuan tertentu. Melalui berbagai cara dan serta jenisnya yang beragam, malware mampu menimbulkan masalah pada perangkat. Berikut merupakan dampak dari serangan malware pada perangkat:
 1. Memperlambat sistem komputer
 2. Kerusakan data dan dokumen
 3. Kendala pada aplikasi di dalamnya
 4. Sistem tidak dapat dibuka
 5. Perubahan data menjadi virus
2. Develop malware trojan dengan Njrat.

Berikut adalah langkah untuk mengembangkan malware trojan dengan Njrat.

 1. Langkah pertama matikan semua software antivirus dan *Firewall* pada kedua komputer yang akan digunakan untuk percobaan njRAT.



2. Install dan ekstrak software njRAT, kemudian jalankan aplikasi njRAT pada komputer host.
3. Jika sudah menjalankan *software* njRAT, maka akan muncul menu awal untuk memasukkan nomer port. Masukkan port 5522.



4. Selanjutnya klik fungsi "Builder" untuk membuat trojan untuk dimasukkan ke PC atau laptop *victim*. Masukkan IP PC atau laptop host, untuk mencari tahu IP device yang digunakan, buka command prompt lalu ketik "ipconfig" lalu klik enter. Jika sudah memasukkan IP address, klik build.

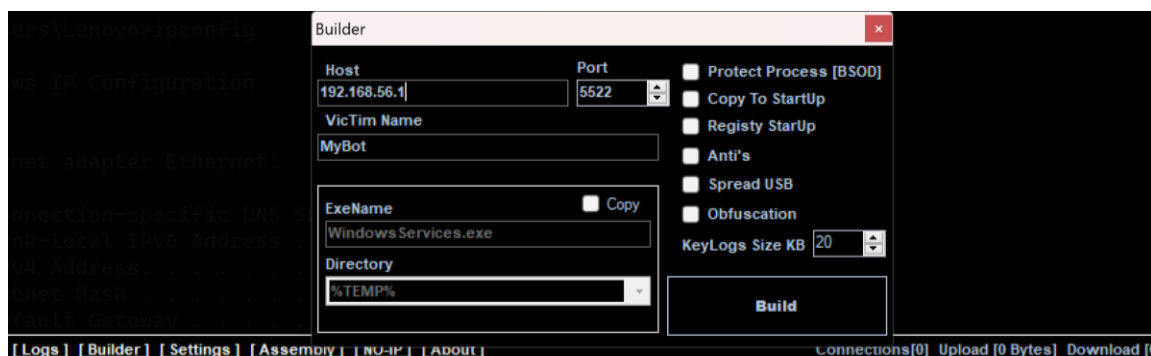
```
Microsoft Windows [Version 10.0.22621.1265]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Lenovo>ipconfig

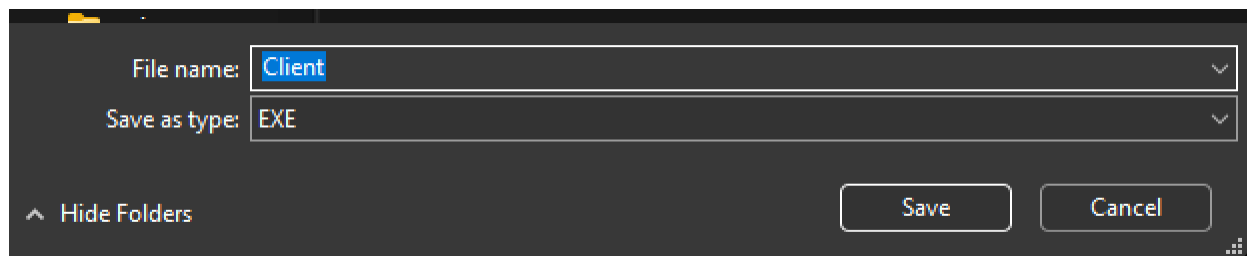
Windows IP Configuration

Ethernet adapter Ethernet:

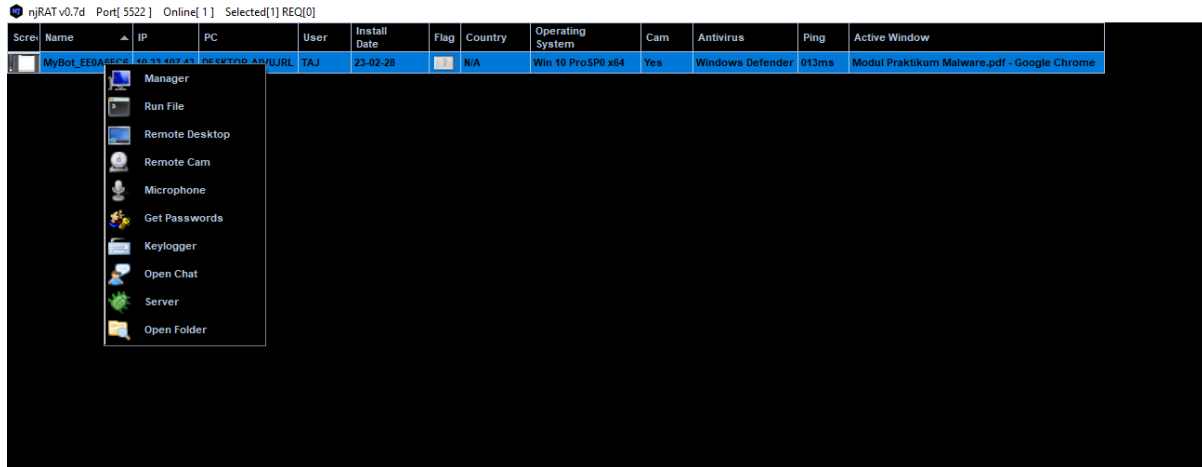
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::8616:4ef8:fc17:8e40%12
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```



5. Simpan file tersebut pada tempat yang diinginkan device host.

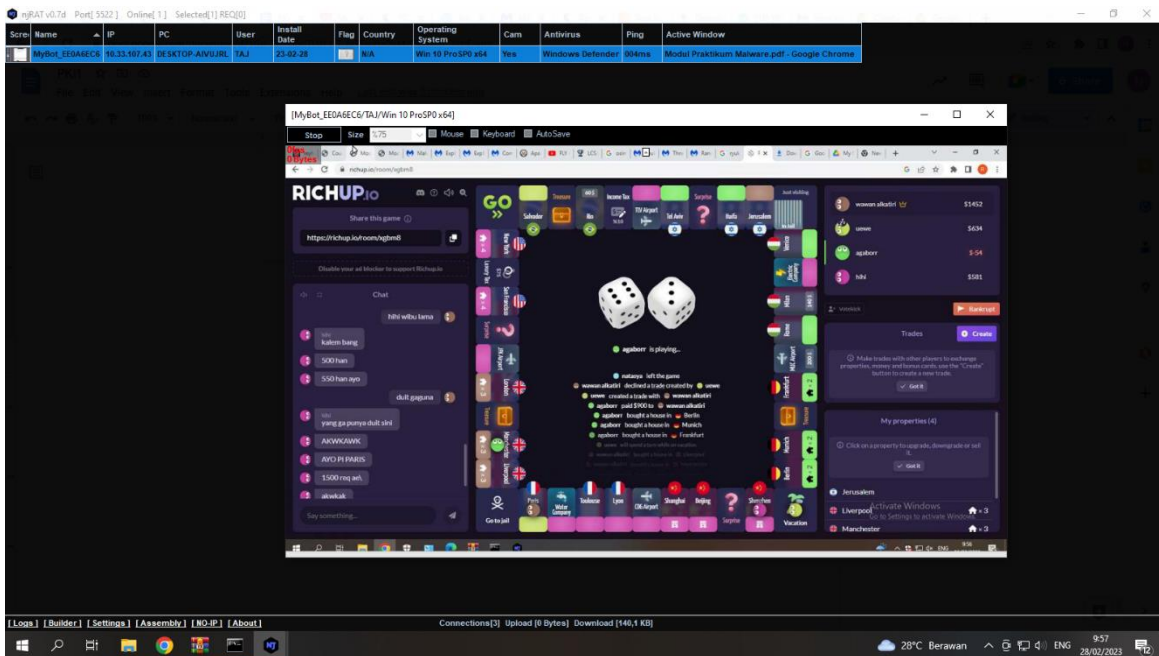


6. Kemudian *copy* hasil file yang sudah dibuat kedalam komputer victim, lalu jalankan pada komputer victim. Akan muncul informasi device victim pada device host. Klik kanan pada victim untuk melihat fungsi yang bisa digunakan.

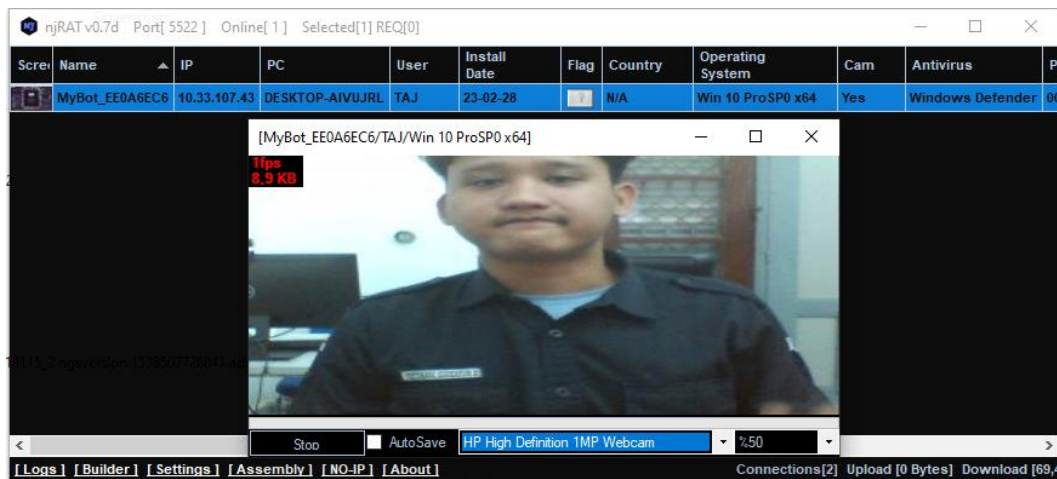


7. Berikut adalah beberapa fungsi njRAT.

a. Remote desktop



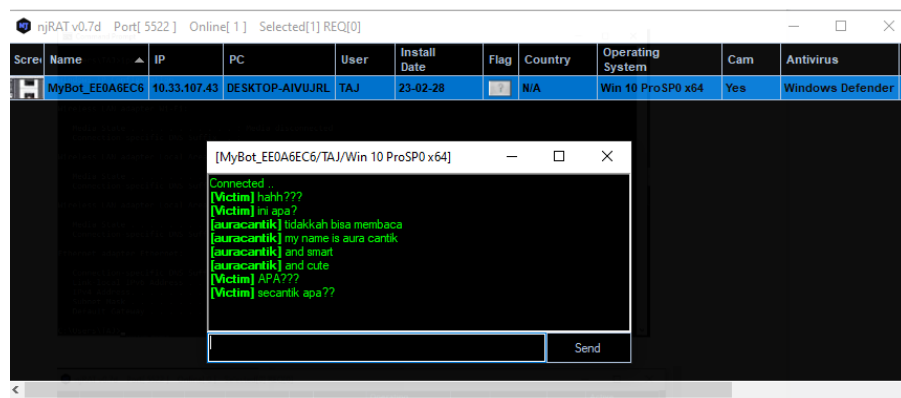
b. Remote cam



c. Keylogger



d. Open chat



3. Analisis malware dengan metode osint:

- Virustotal

The screenshot shows the VirusTotal interface for a file named 'NJRat 0.7D.exe'. The file has a size of 8.54 MB and was uploaded 28 days ago. It has a community score of 54/67, indicating it is malicious. The interface shows various tabs: DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. The 'DETECTION' tab is active, showing a list of security vendors that have flagged the file as malicious. The file is identified as a Trojan, specifically 'Trojan.NJrat.C2464784'.

54 / 67

54 security vendors and no sandboxes flagged this file as malicious

b78fb092e151db613cba51d7f2532547e48c6f4712809a485f272e2ab55776a5

NJrat 0.7D.exe

8.54 MB Size

2023-02-05 16:47:37 UTC 28 days ago

peexe assembly via-tor runtime-modules detect-debug-environment idle spreader direct-cpu-clock-access checks-user-input

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

Popular threat label: trojan.bladabindi/msil

Threat categories: trojan

Family labels: bladabindi msil r014c0d9v22

Security vendors' analysis

Vendor	Detection	Vendor	Detection
Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan.Win32.NJrat.C2464784
Alibaba	Backdoor:MSIL/Bladabindi.41f48f08	ALYac	Trojan.GenericKD.64640381
Antiy-AVL	Trojan.Win32.TSGeneric	Arcabit	Trojan.Generic.D3DA557D
Avast	Win32:KoolhaanX-gen.Trojan	AVG	Win32:KoolhaanX-gen.Trojan

- OPSWAT (Meta Defender)

The screenshot shows the OPSWAT (Meta Defender) interface for a file named 'NJRat 0.7D.exe'. The file has a size of 8.54 MB and was uploaded 28 days ago. It has a community score of 54/67, indicating it is malicious. The interface shows various tabs: Overview, Static Analysis, and Community. The 'Overview' tab is active, showing a list of security vendors that have flagged the file as malicious. The file is identified as a Trojan, specifically 'Trojan.NJrat.C2464784'.

OPSWAT. MetaDefender Cloud

File, URL, IP address, Domain, Hash, or CVE

Process

English Sign In Licensing

Overview

Static Analysis

Community

NJrat 0.7D.exe

Threat name: Trojan/NJrat.C2464784

Cast your vote on this file:

The file is not sanitizable

Metascan

Threats detected

07 / 14 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

- VirSCAN

Please enter the Hash value (support SHA256, SHA1, MD5)

Log in

23 / 46

NjRat 0.7D.exe There are 23 engines checked out

SHA256 : b78fb092e151db613cba51d7f2532547e48c6f4712809a485f272e2ab55776a5

SHA1 : 18602d0db52917b88cbda84ba89181e6fd4686a

MD5 : 70ea9c044c9a766330d3fe77418244a5

file size : 8.54 MB (8954880)

file type : pe

First 2019/07/23 06:12:20 (GMT+7)

commit :

Last 2023/02/28 10:24:14 (GMT+7)

Analysis :

engine detection static information

Last detection time: 2023-02-28 10:24:14

recheck

engine	result	engine	result
AVG	Win32:KeyloggerX-gen	Defenx	Trojan (0048c2571)
Antiy	Trojan/Win32.TSGeneric	Arcabit	Trojan.Generic.D3DA557D
Jiang Min	Backdoor.MSIL.basg	Comodo	Malware @ #1ftda4iuevg4x
Avast	Win32-KeyloggerX-gen	AhnLab	Trojan/Win32 NjRat.C7464784

- 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

This file was scanned a while ago. Below are the results of that scan.

Scan this file again

Name: NjRat 0.7D.exe

Status: Scan finished. 11/14 scanners reported malware.

Size: 8.54MB (8,954,880 bytes)

Scan taken on: February 28, 2023 at 4:27:52 AM GMT+1

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

First seen: September 15, 2018 at 1:49:30 AM GMT+2

MD5: 70ea9c044c9a766330d3fe77418244a5

SHA1: 18602d0db52917b88cbda84ba89181e6fd4686a

Feb 28, 2023 Win32:KeyloggerX-gen

Feb 28, 2023 Found nothing

Feb 28, 2023 MSIL/Generic.APCFB57A01tr

Feb 27, 2023 Trojan.Bladabindi

Feb 27, 2023 Found nothing

Feb 28, 2023 Trojan.GenericKD.64640381

Feb 28, 2023 Found nothing

Feb 27, 2023 Heuristic.HEUR/AGEN.1223243

Feb 28, 2023 Trojan (0048c2571)

Feb 27, 2023 Trojan.MSIL.gen.c.1

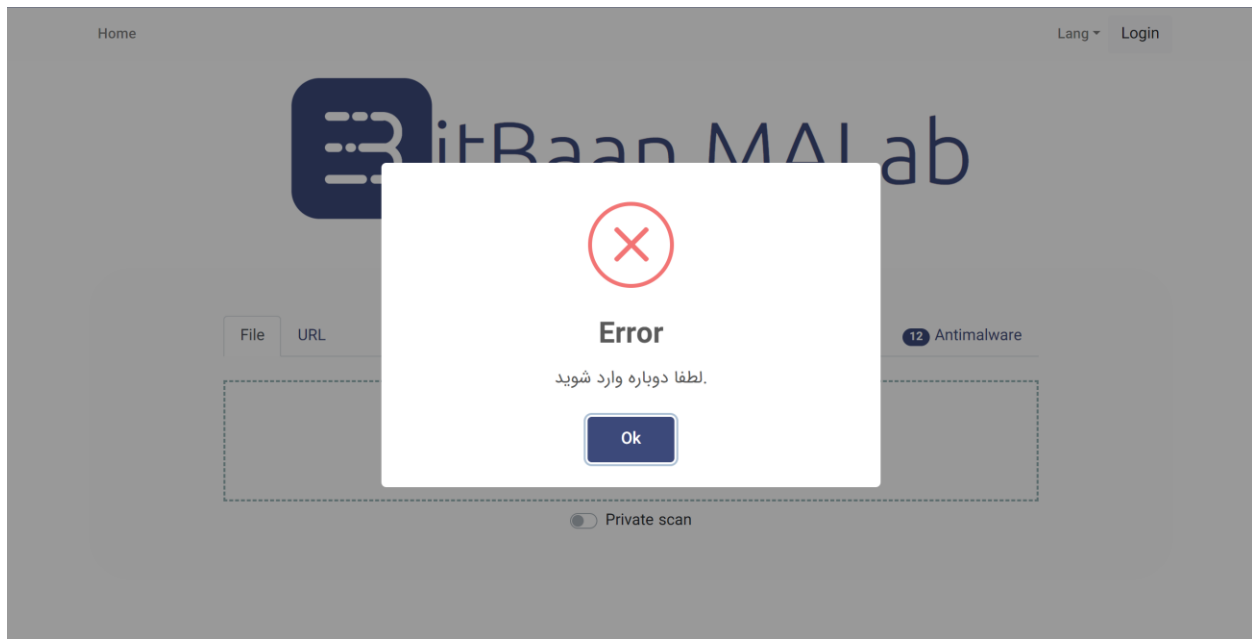
Feb 27, 2023 Win.Malware.Daqc-6598298-0

Feb 28, 2023 Trojan.GenericKD.64640381

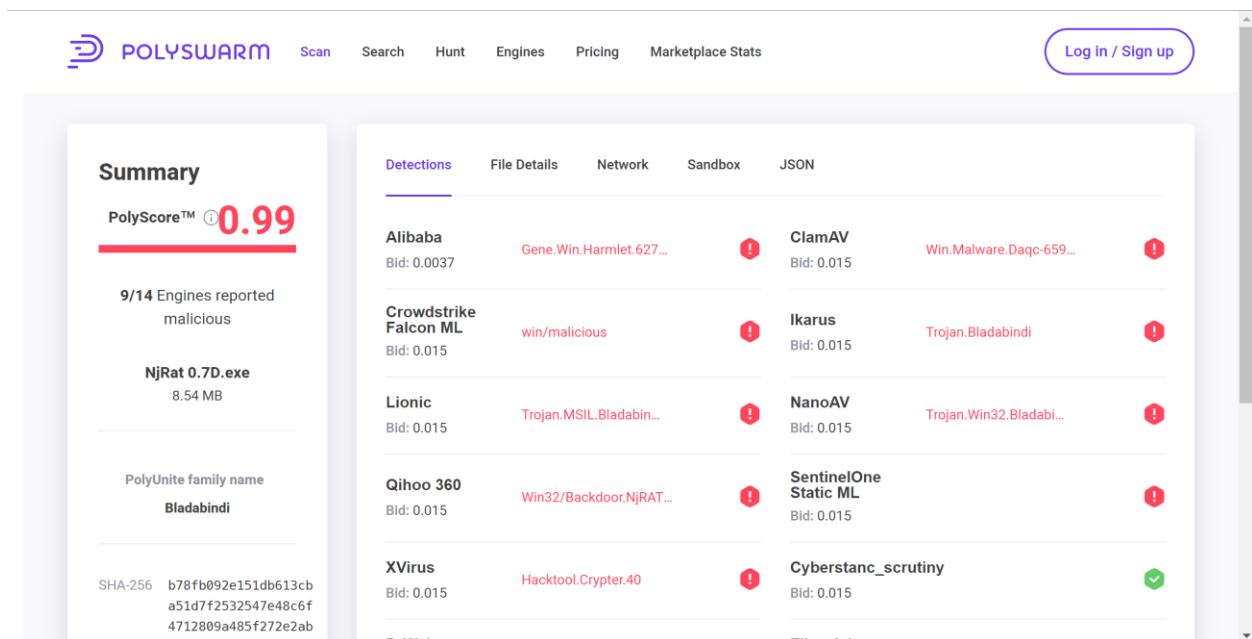
Feb 28, 2023 Trojan.GenericKD.64640381

Feb 28, 2023 HEUR.Backdoor.MSIL.Bladabindi.gen

- Bitbaan MaLab



- PolySwarm



E. Analisis

Praktikum kali ini membahas tentang malware, malware atau *Malicious Software* yang berarti program berbahaya yang dibuat secara khusus untuk menyusup sehingga bisa

tetap berada di dalam sebuah sistem untuk periode waktu tertentu tanpa sepengetahuan pemilik sistem tersebut. Biasanya, malware menyamarkan diri menjadi program yang bersih. Berbagai macam software berbahaya yang dapat ditemukan, terlebih di era dunia digital seperti saat ini. Dengan jenis dan kategori ancaman baru muncul, pengguna harus semakin waspada terhadap jenis malware yang beredar. Sebuah penelitian menemukan bahwa jenis malware yang paling umum sekarang adalah Trojans dan worms. Pada praktikum kali ini kita mencoba menggunakan virus trojan bernama njRAT. Trojan adalah sebuah program jahat yang menyamar menjadi sebuah program yang berguna bagi komputer. Jika korban menginstal trojan pada komputer mereka maka peretas dapat mengakses komputer korban dari jarak jauh. Pada praktikum ini kita mencoba beberapa fitur njRAT, kita bisa mengakses camera dan mikrofon PC/laptop korban, sehingga pelaku dapat memantau korban dari kamera dan mikrofon mereka. Selain mengakses kamera dan mikrofon, pelaku dapat mengambil alih cursor dan keyboard korban. Fitur lain yang dimiliki adalah keylogger yang berfungsi untuk merekam aktivitas pada keyboard komputer korban sehingga pelaku dapat mengetahui apa saja yang diketik oleh korban. Pelaku juga dapat mengakses file-file dan system komputer korban.

Sebagian besar software anti-virus dapat mendeteksi njRAT sebagai trojan sehingga user dapat mengetahui bahwa software yang mereka unduh mengandung file trojan atau tidak. Namun dalam percobaan praktikum, tidak semua software dan web pendeteksi virus dapat mendeteksi file-file berbahaya. Menurut website VirusTotal, hanya 54 dari 67 security vendor dapat mendeteksi bahwa software njRAT berbahaya, dari 14 engine OPSWAT (MetaDefender) hanya 7 yang dapat mendeteksi bahwa njRAT berbahaya. Menurut website VirSCAN, hanya 23 dari 46 engine mereka mampu mendeteksi bahwa njRAT berbahaya. Selanjutnya, website Jotti mengatakan bahwa 3 dari 14 software anti-virus tidak dapat mendeteksi file tersebut berbahaya, kemudian 9 dari 14 engine website PolySwarm mendeteksi bahwa njRAT berbahaya. Tetapi pada website BitBaan MALab tidak bisa melakukan scanning pada software njRAT.

F. Kesimpulan

Kesimpulan yang didapat dari praktikum ini adalah:

1. Sebuah virus tidak dapat 100% terdeteksi oleh software maupun website pendeteksi anti-virus. Namun pengguna dapat mengamankan perangkat dari deteksi dari software maupun website pendeteksi anti-virus
2. 1 antivirus software dapat mendeteksi sebagian besar virus yang ada di internet.
3. Malware adalah perangkat lunak yang dibuat dengan tujuan memasuki dan terkadang merusak sistem komputer, jaringan, atau server tanpa diketahui oleh pemiliknya.

G. Daftar Pustaka

Dewaweb Team. 2022. *Apa itu Malware? Pengertian, Jenis dan Cara Mengatasinya*. Diakses pada 6 Maret 2023. <https://www.dewaweb.com/blog/pengertian-malware-pentingnya-dewaguard/>

Shinra, Amelia. 2023. *Ketahui Apa itu Trojan, Jenisnya dan Cara Menghindarinya*. Diakses pada 6 Maret 2023. <https://www.dewaweb.com/blog/apa-itu-trojan/#:~:text=Trojan%20adalah%20malware%20yang%20memasuki%20sistem%20dengan%20cara,berbahaya.%20Trojan%20juga%20dikenal%20dengan%20nama%20Trojan%20Horse.>