LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1
Unit 4 – Analisis Malware

DI SUSUN OLEH

Nama	: M Abdul Aziz
NIM	: 21/474516/SV/18951
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
Unit 4 – Analisis Malware

I. Tujuan

– Meneliti dan menganalisis malware

II. Landasan Teori

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 diupload 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. 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 :

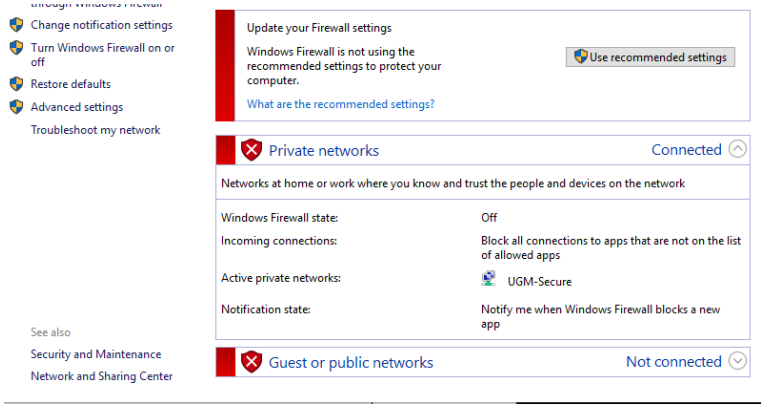
- *Screen/camera capture atau control*
- *File management (download/upload/execute/dll.)*
- *Shell control (CMD control) Computer control (power off/on/log off)*
- *Registry management (query/add/delete/modify)*
- *Password management.*

III. Alat & Bahan

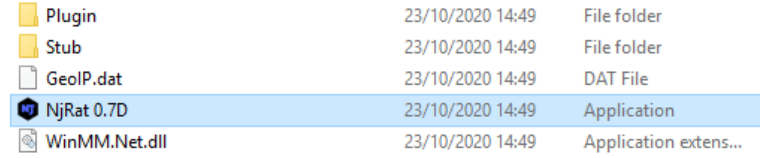
– Laptop/PC
– Software NJRAT
– Koneksi Internet

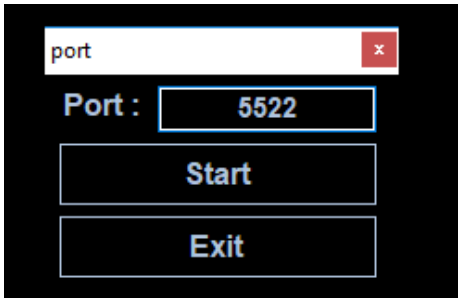
IV. Instruksi Kerja

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 firewall pada PC

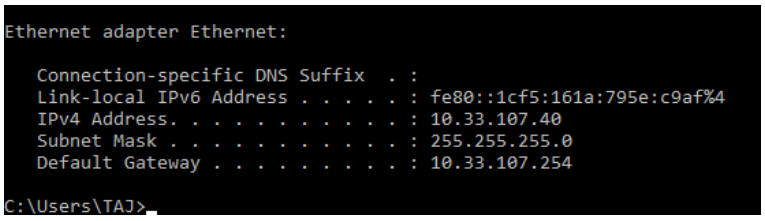


5. Download dan ekstrak aplikasi NJRAT kemudian run aplikasi NJRAT pada komputer host. File dapat di download di https://github.com/adarift/njRAT/releases/tag/v0.7D. Masukkan port yang ingin digunakan, misal 5522



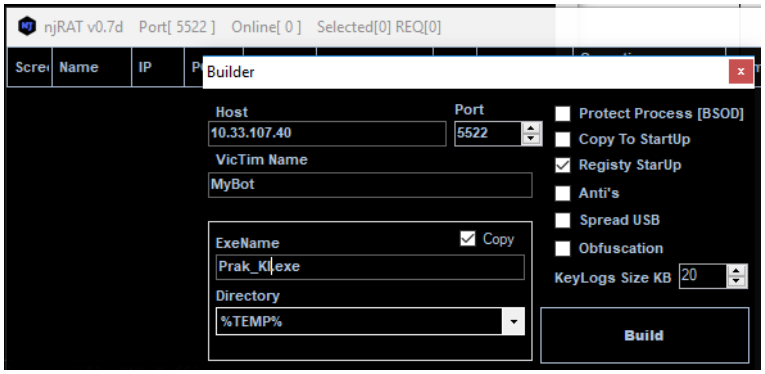


6. Kemudian cek IP Address host (PC/Laptop) terlebih dahulu. IP ini nantinya akan digunakan oleh NJRAT, dan pastikan juga komputer victim berada pada satu jaringan.

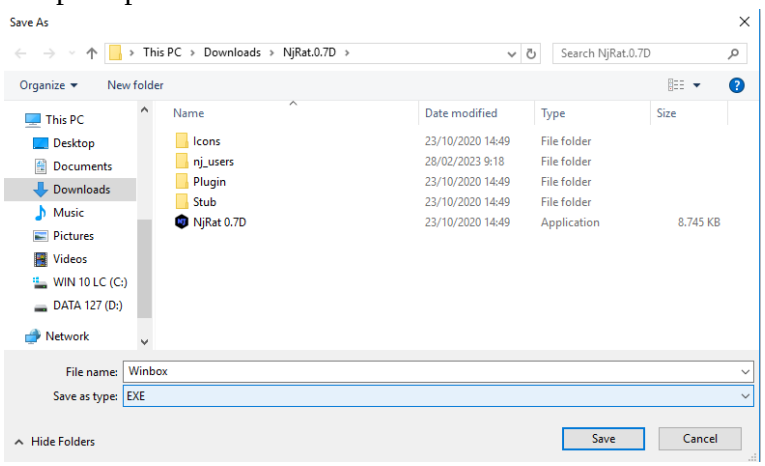


7. Buat aplikasi yang akan dipasang pada komputer victim. Masukkan IP Address host pada kolom host dan port yang sesuai dengan yang kita tentukan tadi pada

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

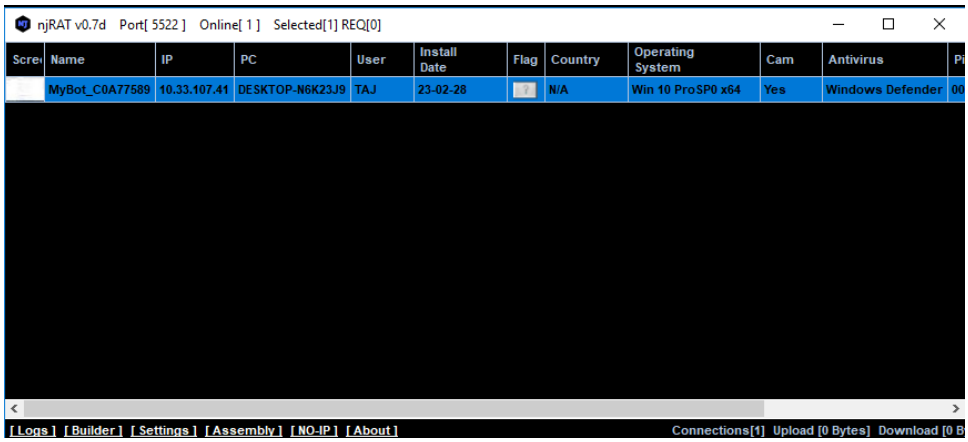


8. Simpan aplikasi hasil build



9. Kemudian, copykan aplikasi Winbox.exe yang sudah telah kita buat ke dalam komputer victim. Kemudian, pada komputer victim jalankan aplikasi tersebut.

10. Ketika sudah terpasang pada komputr victim, NJRAT pada host akan mendeteksi komputer victim



V. Hasil & Pembahasan

- **Analisis Anatomy Malware**

1. Contoh-contoh malware

a. Keylogger

Keylogger adalah metode peretasan yang dilakukan dengan cara merekam aktivitas keyboard komputer secara diam-diam. Serangan ini berbentuk spyware atau perangkat lunak berbahaya yang biasanya dilampirkan pada email. Jika spyware terpasang pada komputer, maka hacker bisa merekam setiap keystroke pada keyboard perangkat komputer tersebut.

b. Botnet

Botnet adalah sekumpulan program yang terinfeksi malware dan terhubung dalam jaringan internet yang dikendalikan oleh pihak tertentu. Istilah botnet merupakan singkatan dari robot dan network. Bisa dibilang, botnet adalah kumpulan bot yang dirancang untuk bisa dijalankan otomatis pada sebuah jaringan dan dikendalikan dari jarak jauh.

Pelaku akan mengumpulkan bot sebanyak-banyaknya untuk digabungkan menjadi sebuah jaringan bot. Bot dibentuk dari komputer-komputer yang diinfeksi malware dan dikendalikan oleh botmaster. Jika sebuah komputer telah terinfeksi botnet, maka saat tersambung ke jaringan, komputer tersebut akan menjalankan perintah apapun yang diberikan botmaster. Semakin banyak resource bot yang dimiliki, maka serangan kejahatan akan semakin kuat.

c. 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.

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.

d. Spyware

Spyware adalah salah satu ancaman paling umum bagi pengguna internet. Setelah diinstal, ia memantau aktivitas internet, melacak kredensial login, dan memata-matai informasi sensitif. Tujuan utama dari

spyware biasanya untuk mendapatkan nomor kartu kredit, informasi perbankan dan password.

2. Analisis malware

Dari beberapa malware yang telah disebutkan, botnet merupakan salah satu malware yang sering muncul di jaringan internet. Contohnya adalah *phising* yang sering muncul dalam suatu laman web. Botnet ini dibentuk dari komputer-komputer yang diinfeksi *malware* dan dikendalikan oleh botmaster. Jika sebuah komputer telah terinfeksi botnet, maka saat tersambung ke jaringan, komputer tersebut akan menjalankan perintah apapun yang diberikan botmaster. Semakin banyak resource bot yang dimiliki, maka serangan kejahatan akan semakin kuat.

Cara penularan dari malware ini kebanyakan dari *social enggineering* agar pengguna mengunduh virus Trojan. Selanjutnya *hacker* akan mengambil alih kontrol setiap komputer yang sudah terinfeksi. Botmaster akan mengatur semua bot menjadi botnet dan mengendalikannya dari jauh. Umumnya, botmaster akan menginfeksi jutaan komputer aktif untuk memperkuat bot.

Bagi komputer yang disusupi untuk membentuk jaringan botnet, dampak serangan tidak akan terlalu merugikan. Hal ini karena kebanyakan botmaster menginfeksi komputer hanya untuk memperkuat botmaster. Namun dampak/kerugian akan dirasakan oleh target sebenarnya, atau biasa disebut *next target*. Dampak yang dirasakan diantaranya adalah Performa jaringan menurun drastis dan kecepatan internet akan melemah, Performa perangkat/komputer juga akan menurun, Menguras banyak bandwith karena digunakan untuk mengunduh informasi yang dibutuhkan botnet, dan Melumpuhkan sistem komputer sehingga tidak dapat beroperasi lagi.

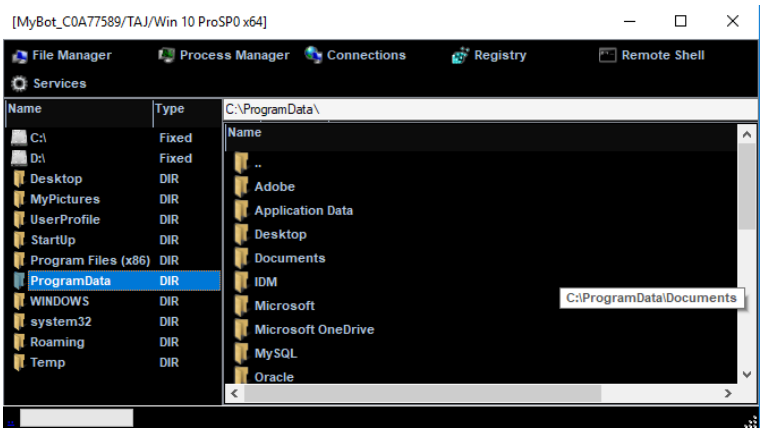
- **Praktikum NJRAT**

Pada praktikum ini, mahasiswa diminta untuk *developing malware* menggunakan NJRAT. Sebelumnya, agar *software* dapat dijalankan maka perlu mematikan *windows seurity* terlebih dahulu. Jika *windows security* tidak dimatikan, maka windows akan mendeteksi bahwa *software* NJRAT merupakan *software* berbahaya, sehingga *software* tidak dapat di-*download* maupun di-*install*.

Setelah *software* NJRAT telah di-*install*, selanjutnya adalah *build* aplikasi yang akan di *install* di komputer korban. Sebelumnya, masukan terlebih dahulu IP *Address* dari PC/Host yang digunakan serta port yang ingin digunakan. Kemudian pastikan host dalam satu jaringan dengan komputer korban, karena hal ini hanya digunakan untuk pengujian yang berada dalam

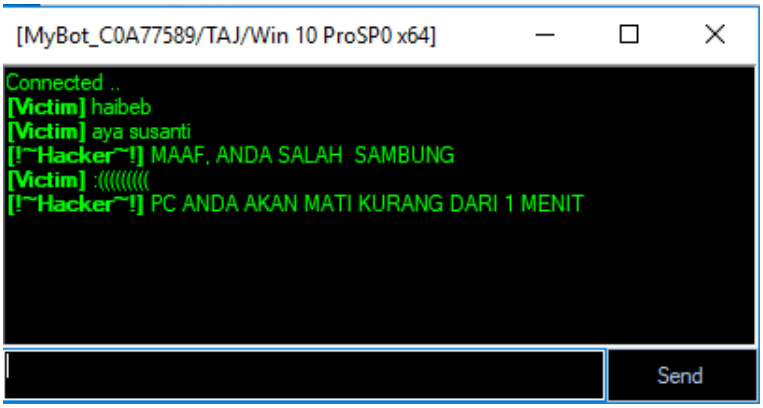
jaringan lokal. Setelah file aplikasi berhasil dibuat, jalankan aplikasi tersebut di komputer korban dan pastikan host telah mendeteksi komputer korban.

Kemudian lakukan beberapa pengujian seperti *remote camera*, *remote file manager*, serta *chat message*. Berikut merupakan hasil pengujian yang telah dilaksanakan pada praktikum ini.



Gambar Hasil Pengujian *remote file manager*

Gambar Hasil Pengujian *remote camera*

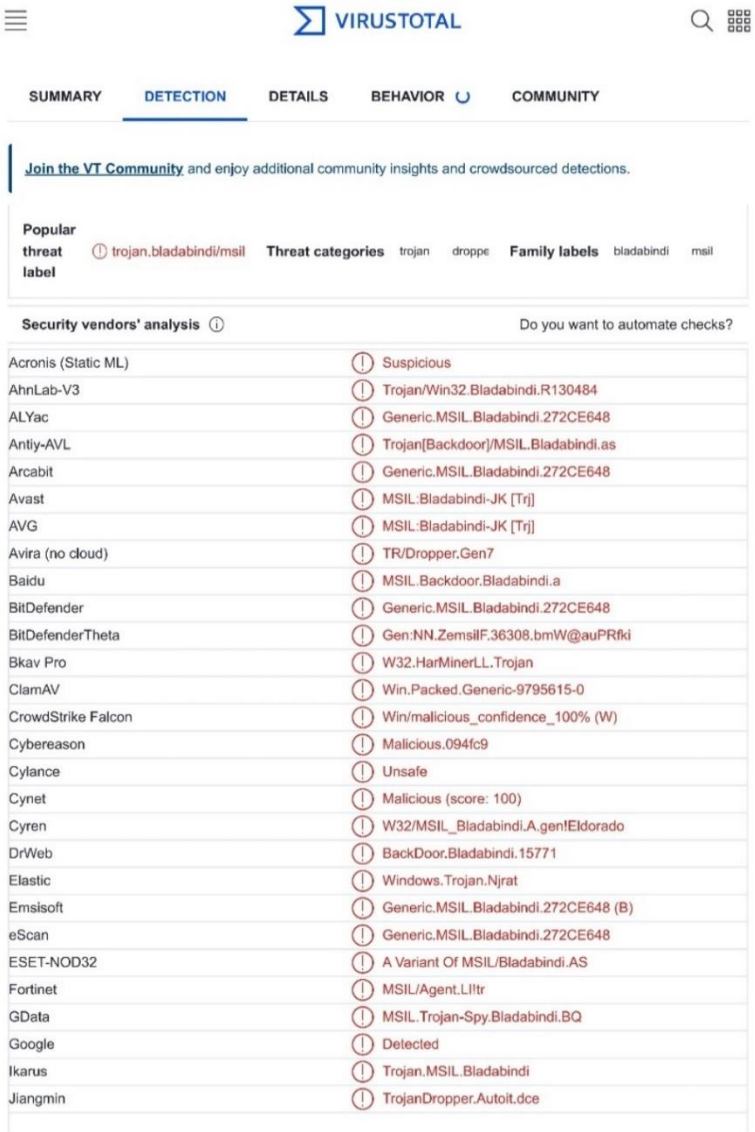


Gambar Hasil Pengujian *chat message*

Dari hasil praktikum ini, dapat dilihat bahwa penyebaran malware ini menggunakan teknik *social engineering*, dimana korban akan diarahkan untuk menginstall file aplikasi yang berisi malware. Setelah korban menginstall file tersebut, penyerang dapat melakukan apapun yang diinginkan tanpa sepengetahuan korban.

- **Analisis malware dengan metode OSINT**

  a. VirusTotal



VIRUSTOTAL

SUMMARY | DETECTION | DETAILS | BEHAVIOR | COMMUNITY

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

Popular threat label: trojan.bladabindi/msil | Threat categories: trojan, droppe | Family labels: bladabindi, msil

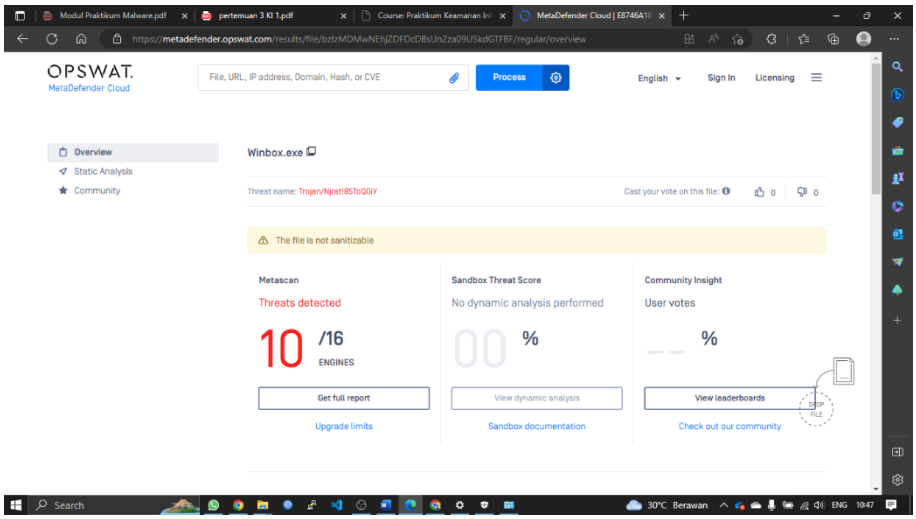
Security vendors' analysis — Do you want to automate checks?

Acronis (Static ML)	Suspicious
AhnLab-V3	Trojan/Win32.Bladabindi.R130484
ALYac	Generic.MSIL.Bladabindi.272CE648
Antiy-AVL	Trojan[Backdoor]/MSIL.Bladabindi.as
Arcabit	Generic.MSIL.Bladabindi.272CE648
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.272CE648
BitDefenderTheta	Gen:NN.ZemsilF.36308.bmW@auPRfki
Bkav Pro	W32.HarMinerLL.Trojan
ClamAV	Win.Packed.Generic-9795615-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.094fc9
Cylance	Unsafe
Cynet	Malicious (score: 100)
Cyren	W32/MSIL_Bladabindi.A.gen!Eldorado
DrWeb	BackDoor.Bladabindi.15771
Elastic	Windows.Trojan.Njrat
Emsisoft	Generic.MSIL.Bladabindi.272CE648 (B)
eScan	Generic.MSIL.Bladabindi.272CE648
ESET-NOD32	A Variant Of MSIL/Bladabindi.AS
Fortinet	MSIL/Agent.LI!tr
GData	MSIL.Trojan-Spy.Bladabindi.BQ
Google	Detected
Ikarus	Trojan.MSIL.Bladabindi
Jiangmin	TrojanDropper.Autoit.dce

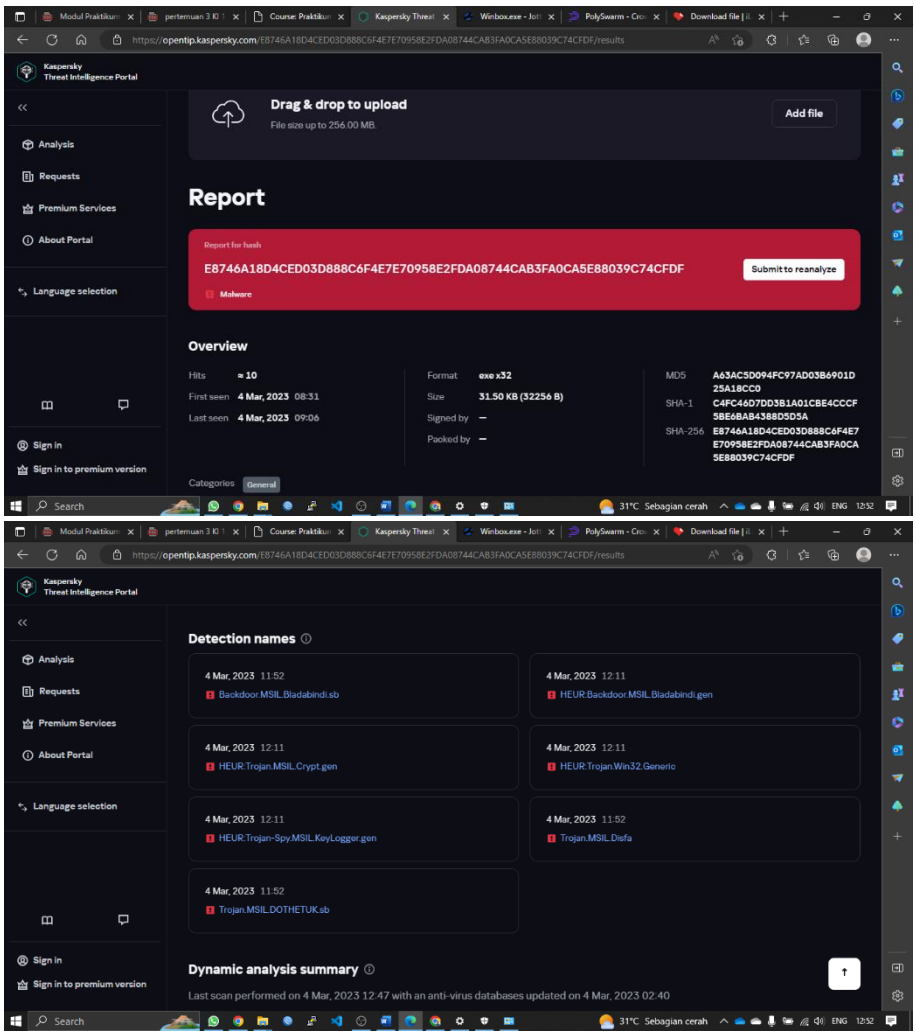
K7AntiVirus	Trojan (700000121)
K7GW	Trojan (700000121)
Kaspersky	HEUR:Trojan.Win32.Generic
Malwarebytes	Bladabindi.Backdoor.Bot.DDS
MAX	Malware (ai Score=83)
MaxSecure	Trojan.Malware.300983.susgen
McAfee	BackDoor-NJRat!A63AC5D094FC
McAfee-GW-Edition	BehavesLike.Win32.BackdoorNJRat.nm
Microsoft	Backdoor:MSIL/Bladabindi
NANO-Antivirus	Trojan.Win32.Gen8.ecsqgn
QuickHeal	Trojan.GenericFC.S20328680
Rising	Backdoor.njRAT!1.9E49 (CLASSIC)
Sangfor Engine Zero	Suspicious.Win32.Save.a
SecureAge	Malicious
SentinelOne (Static ML)	Static AI - Malicious PE
Sophos	Mal/Bladabi-D
Symantec	MSIL.Trojan!gen2
TACHYON	Backdoor/W32.DN-NjRat.32256
Tencent	Trojan.Msil.Bladabindi.fb
Trapmine	Malicious.high.ml.score
Trellix (FireEye)	Generic.mg.a63ac5d094fc97ad
TrendMicro	BKDR_BLADABI.SMC
VBA32	Trojan.MSIL.Bladabindi.Heur
VIPRE	Generic.MSIL.Bladabindi.272CE648
VirIT	Trojan.Win32.Dnldr25.DDDI
Xcitium	Backdoor.MSIL.Bladabindi.BA@7oej5x
Yandex	Trojan.AvsMofer.dd6520
Zillya	Trojan.Bladabindi.Win32.99364
Zoner	Trojan.Win32.85838
Alibaba	Undetected
CMC	Undetected
F-Secure	Undetected
Gridinsoft (no cloud)	Undetected
Lionic	Undetected
Palo Alto Networks	Undetected
Panda	Undetected
SUPERAntiSpyware	Undetected
TEHTRIS	Undetected
TrendMicro-HouseCall	Undetected
ViRobot	Undetected
Webroot	Undetected

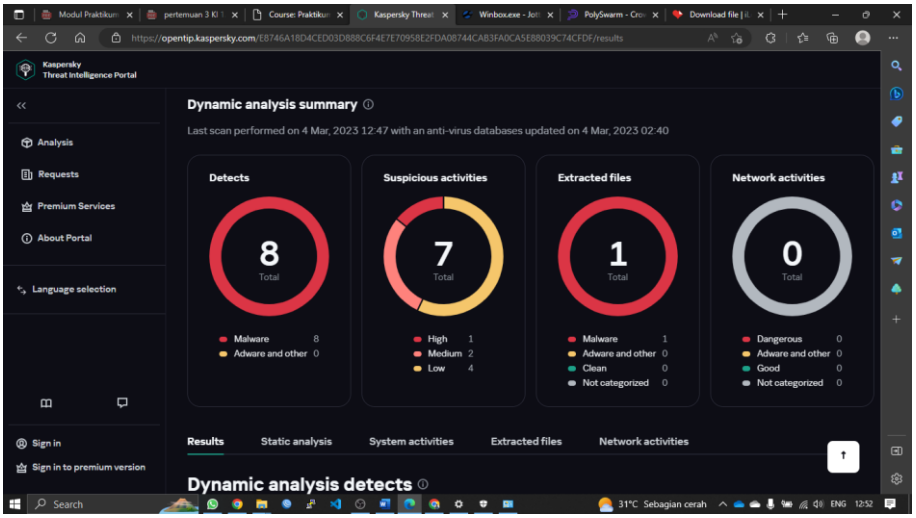
ZoneAlarm by Check Point	Undetected
Avast-Mobile	Unable to process file type
BitDefenderFalx	Unable to process file type
Symantec Mobile Insight	Unable to process file type
Trustlook	Unable to process file type

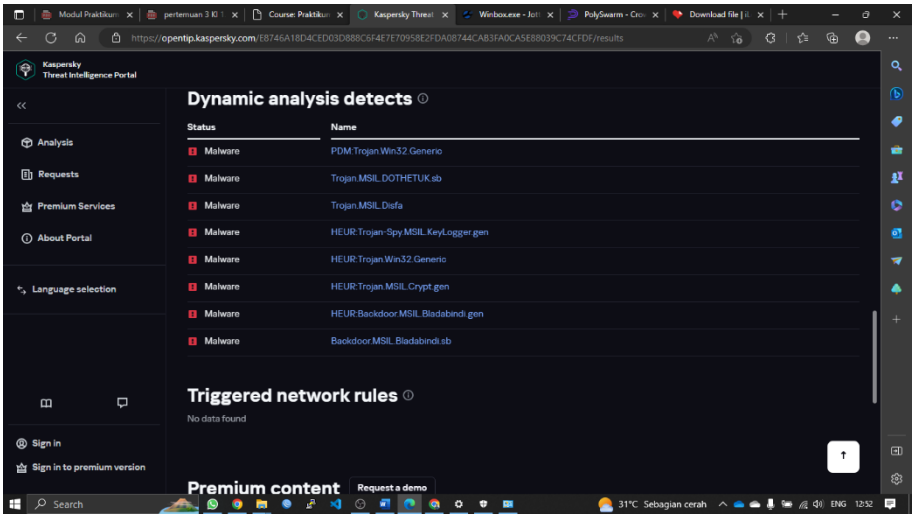
b. OPSWAT (*Meta Defender*)



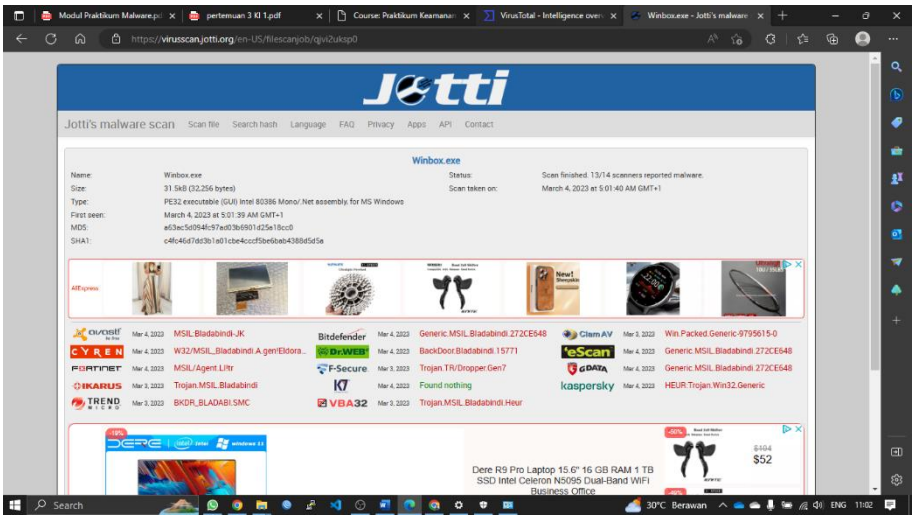
c. VirSCAN



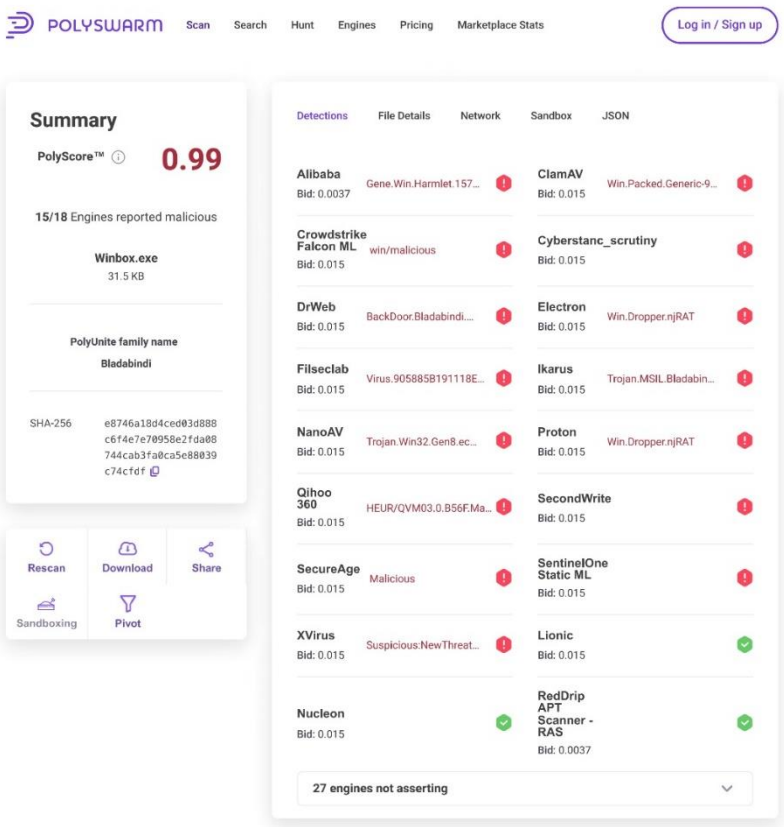

Kaspersky Threat Intelligence Portal
Dynamic analysis summary
Last scan performed on 4 Mar, 2023 12:47 with an anti-virus databases updated on 4 Mar, 2023 02:40
Detects
8
Total
Malware 8
Adware and other 0
Suspicious activities
7
Total
High 1
Medium 2
Low 4
Extracted files
1
Total
Malware 1
Adware and other 0
Clean 0
Not categorized 0
Network activities
0
Total
Dangerous 0
Adware and other 0
Good 0
Not categorized 0
Results
Static analysis
System activities
Extracted files
Network activities
Dynamic analysis detects
Analysis
Requests
Premium Services
About Portal
Language selection
Sign in
Sign in to premium version


Kaspersky Threat Intelligence Portal
Dynamic analysis detects
Status
Name
Malware PDM:Trojan.Win32.Generic
Malware Trojan.MSIL.DOTHETUK.sb
Malware Trojan.MSIL.Disfa
Malware HEUR:Trojan-Spy.MSIL.KeyLogger.gen
Malware HEUR:Trojan.Win32.Generic
Malware HEUR:Trojan.MSIL.Crypt.gen
Malware HEUR:Backdoor.MSIL.Bladabindi.gen
Malware Backdoor.MSIL.Bladabindi.sb
Triggered network rules
No data found
Premium content
Request a demo
Analysis
Requests
Premium Services
About Portal
Language selection
Sign in
Sign in to premium version

d. Jotti


Jotti
Jotti's malware scan
Winbox.exe
Bitdefender
Dr.WEB
F-Secure
K7
VBA32
ClamAV
eScan
GDATA
kaspersky
Dere R9 Pro Laptop 15.6" 16 GB RAM 1 TB SSD Intel Celeron N5095 Dual-Band WIFI Business Office
$52

e. Polyswarm



f.

Seperti yang ditunjukkan pada hasil *scanning malware* dari file malware yang telah dibuat menggunakan *software* NJRAT, terdapat beberapa perbedaan hasil dari *scanning* pada setiap *tools* yang digunakan. Berikut merupakan tabel hasil *scanning* malware dari setiap *tools* OSINT yang digunakan.

NO	OSINT *Tools*	Hasil *Scanning*
1	VirusTotal	60/73
2	OPSWAT (*Meta Defender)*	10/16
3	VirSCAN	16
4	Jotti	13/14
5	Polyswarm	15/18

Tabel hasil *scanning* dengan *tools* OSINT

Pada bagian ini, mirip dengan VirusTotal, OSINT lain digunakan untuk mengidentifikasi berapa banyak mesin yang dapat mendeteksi malware agar terdapat data dari sumber lain. Seperti hasil yang ditunjukkan pada tabel, setelah terdapat beberapa perbedaan hasil *scanning malware* dari seriap *tools* yang digunakan. Ini menandakan bahwa terdapat perbedaan yang sangat efektif

dan kuat karena terdapat perbedaan dalam hasilnya. Dari hasil tersebut pula, VirSCAN juga memberikan banyak informasi lain mengenai enkripsi yang terdapat dalam malware tersebut seperti MD5, SHA-1, SHA-256, nilai Vhash, dll. Demikian pula, OSINT lain juga memberikan informasi yang sama bahkan terdapat juga informasi yang lebih banyak tentang file.

VI. Kesimpulan

Pada praktikum kali ini dapat disimpulkan bahwa :

1. NJRAT merupakan software untuk *developing* malware jenis Trojan.
2. NJRAT berjalan menggunakan teknik *Social Engineering*.
3. Malware Trojan berjalan tanpa sepengetahuan korban.
4. OSINT digunakan untuk mengetahui informasi *malware* yang terdapat dalam sebuah aplikasi yang tidak terdapat dalam tool OSINT lain.

VII. Daftar Pustaka

Cloudmatika. (December 24, 2022). 10 Jenis-Jenis Malware yang Dapat Mengancam Data Perusahaan Anda. Retrieved March 06, 2023, from https://www.cloudmatika.co.id/blog-detail/jenis-jenis-malware

Huda, N. (September 02, 2022). Pengertian Keylogger, Cara Kerja, Jenis dan Cara Menghindarinya. Retrieved March 06, 2023, from https://www.dewaweb.com/blog/pengertian-keylogger/#Apa_itu_Keylogger

Shinta, A. (May 17, 2022). Kenali Apa itu Botnet, Jenis dan Cara Menghindarinya. Retrieved March 06, 2023, from https://www.dewaweb.com/blog/apa-itu-botnet/

Kuncoro, A. A. (March 30, 2022). Worm Komputer. Retrieved March 06, 2023, from http://teknik-informatika-s1.stekom.ac.id/informasi/baca/Worm-Komputer/441b7d76c787c5c38ca3b5f48f1c3aadc82adf18

Fauziah, N. (March 30, 2022). Spyware – Pengertian, Jenis, dan Cara Terbaik Melindungi Komputer Anda!. Retrieved March 06, 2023, from https://academy.alterra.id/blog/spyware-adalah/