

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 :

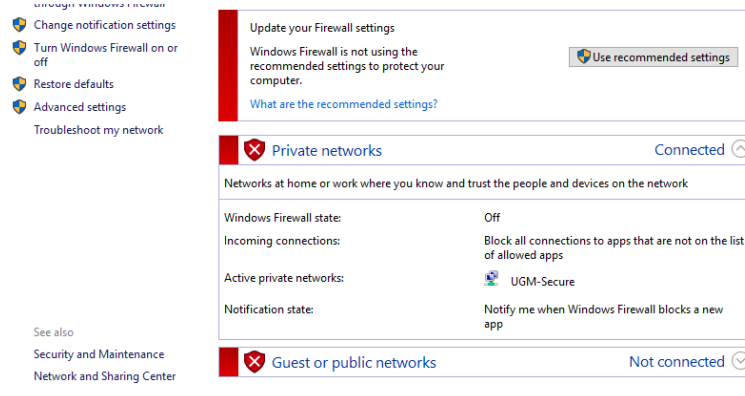
- *Screen/camera capture atau control*
- *File management (download/upload/execute/dll.)*
- *Shell control (CMD control) Computer control (power off/on/log off)*
- *Registry management (query/add/delete/modify)*
- *Password management.*

III. Alat & Bahan

- Laptop/PC
- Software NJRAT
- Koneksi Internet

IV. Instruksi Kerja

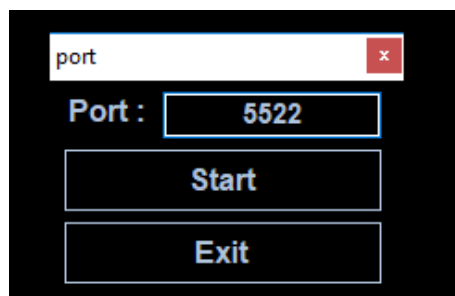
1. Menggunakan mesin pencari favorit Anda, lakukan pencarian untuk malware terbaru. Selama pencarian Anda, pilih empat contoh malware, masing-masing dari jenis malware yang berbeda, dan bersiaplah untuk membahas detail tentang apa yang dilakukan masing-masing, bagaimana masing-masing ditransmisikan, 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





- 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

Plugin	23/10/2020 14:49	File folder
Stub	23/10/2020 14:49	File folder
GeoIP.dat	23/10/2020 14:49	DAT File
NjRat 0.7D	23/10/2020 14:49	Application
WinMM.Net.dll	23/10/2020 14:49	Application extens...



- 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.

```

Ethernet adapter Ethernet:

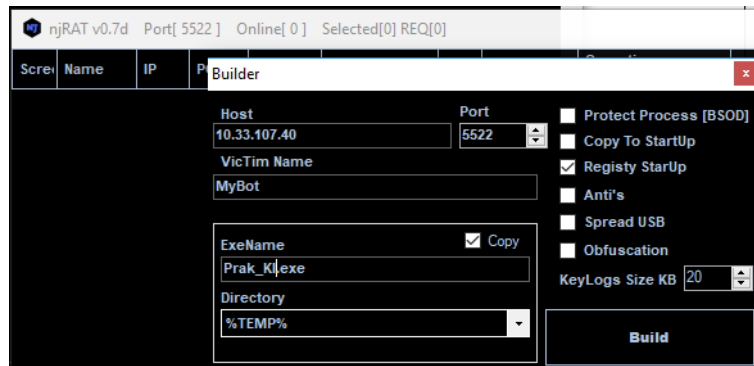
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::1cf5:161a:795e:c9af%4
    IPv4 Address. . . . . : 10.33.107.40
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.33.107.254

C:\Users\TAJ>

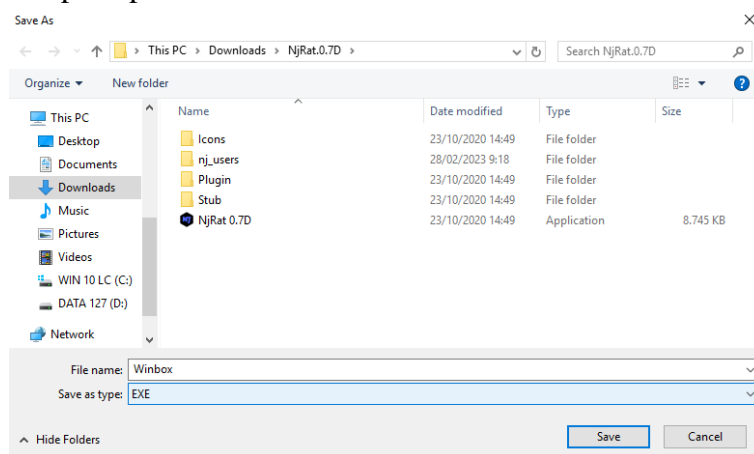
```

- 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 keamanan 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

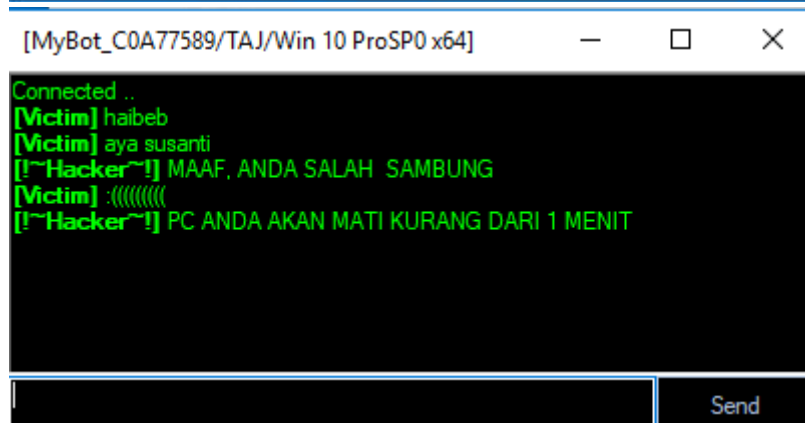
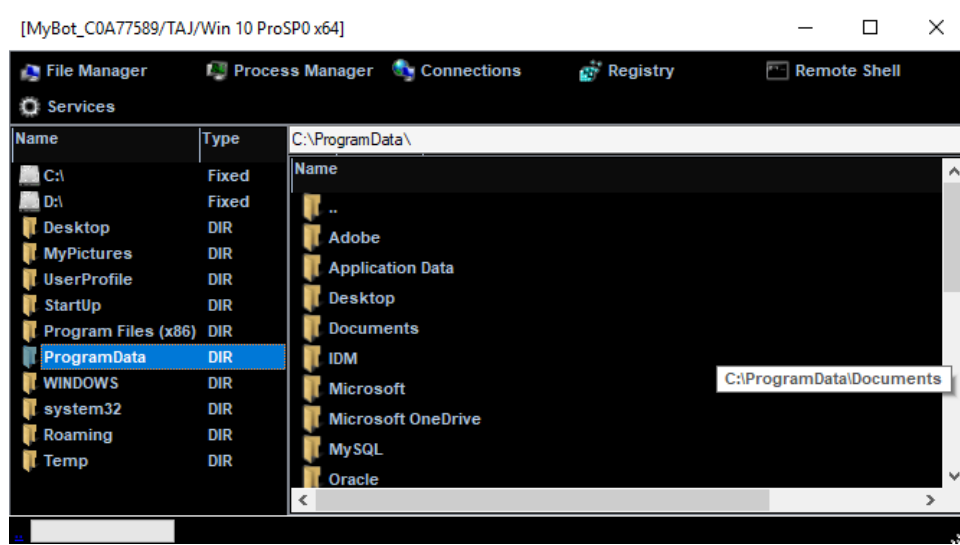
Dari beberapa malware yang telah disebutkan, botnet merupakan salah satu malware yang sering muncul di jaringan internet. Contohnya adalah *phishing* yang sering muncul dalam suatu laman web. Botnet ini dibentuk dari komputer-komputer yang diinfeksi *malware* dan dikendalikan oleh botmaster. Jika sebuah 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 engineering* 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 bandwidth 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 security* terlebih dahulu. Hal ini karena *software* NJRAT sendiri akan terdeteksi JikaJikaJika *windows security* tidak dimatikan, maka windows akan mendeteksi bahwa *software* NJRAT merupakan *software* berbahaya



- Analisis malware dengan metode OSINT
 - a. VirusTotal



Join the [VT Community](#) and enjoy additional community insights and crowdsourced detections.

Popular

threat

[trojan.bladabindi/msil](#)

label

Threat categories

[trojan](#)[dropper](#)

Family labels

[bladabindi](#)[msil](#)

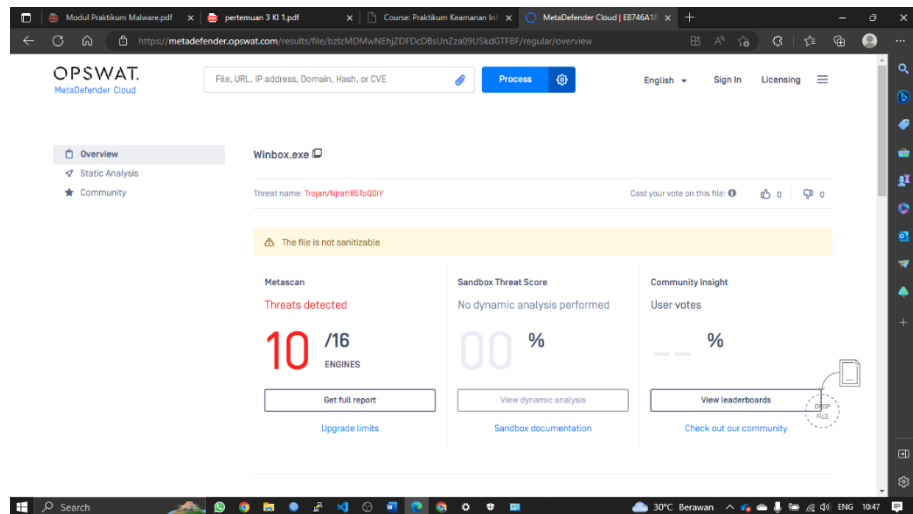
Security vendors' analysis

Do you want to automate checks?

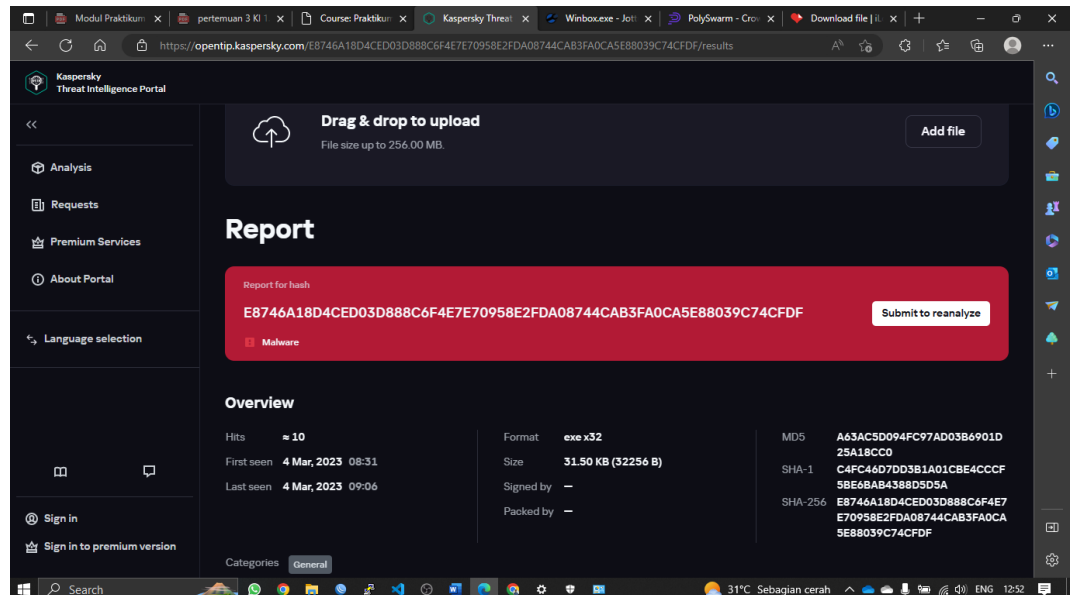
Acronis (Static ML)	Suspicious
AhnLab-V3	Trojan/Win32.Bladabindi.R130484
ALYac	Generic.MSIL.Bladabindi.272CE648
Antiy-AVL	Trojan[Backdoor]/MSIL.Bladabindi.as
Arcabit	Generic.MSIL.Bladabindi.272CE648
Avast	MSIL.Bladabindi-JK [Trj]
AVG	MSIL.Bladabindi-JK [Trj]
Avira (no cloud)	TR/Dropper.Gen7
Baidu	MSIL.Backdoor.Bladabindi.a
BitDefender	Generic.MSIL.Bladabindi.272CE648
BitDefenderTheta	Gen:NN.ZemslF.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.L!ltr
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-NJRa!A63AC5D094FC
McAfee-GW-Edition	⚠ BehavesLike.Win32.BackdoorNJRa!.nm
Microsoft	⚠ Backdoor:MSIL/Bladabindi
NANO-Antivirus	⚠ Trojan.Win32.Gen8.ecsqgn
QuickHeal	⚠ Trojan.GenericFC.S20328680
Rising	⚠ Backdoor.njRa!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-NjRa.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



Modul Praktikum x pertemuan 3 KI 1 x Course: Praktikum x Kaspersky Threat x Winbox.exe - Joti x PolySwarm - Cro x Download file | x

https://opentip.kaspersky.com/E8746A18D4CED03D888C6F4E7E70958E2FDA08744CAB3FA0CA5E88039C74CFDF/results

Kaspersky
Threat Intelligence Portal

<<

Analysis

Requests

Premium Services

About Portal

Language selection

Sign in

Sign in to premium version

Detection names ⓘ

4 Mar, 2023 11:52
Backdoor.MSIL.Bladabindi.sb

4 Mar, 2023 12:11
HEUR:Backdoor.MSIL.Bladabindi.gen

4 Mar, 2023 12:11
HEUR:Trojan.MSIL.Crypt.gen

4 Mar, 2023 12:11
HEUR:Trojan.Spy.MSIL.KeyLogger.gen

4 Mar, 2023 11:52
Trojan.MSIL.Disfa

4 Mar, 2023 11:52
Trojan.MSIL.DOTHETUK.sb

Dynamic analysis summary ⓘ

Last scan performed on 4 Mar, 2023 12:47 with an anti-virus databases updated on 4 Mar, 2023 02:40

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

Good 0

Not categorized 0

Results

Static analysis

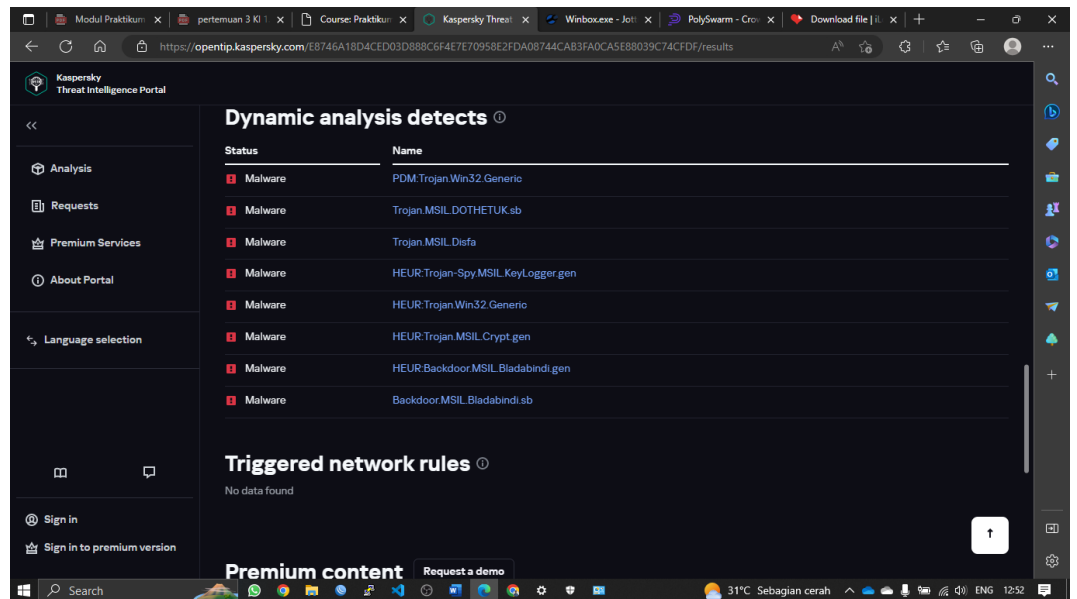
System activities

Extracted files

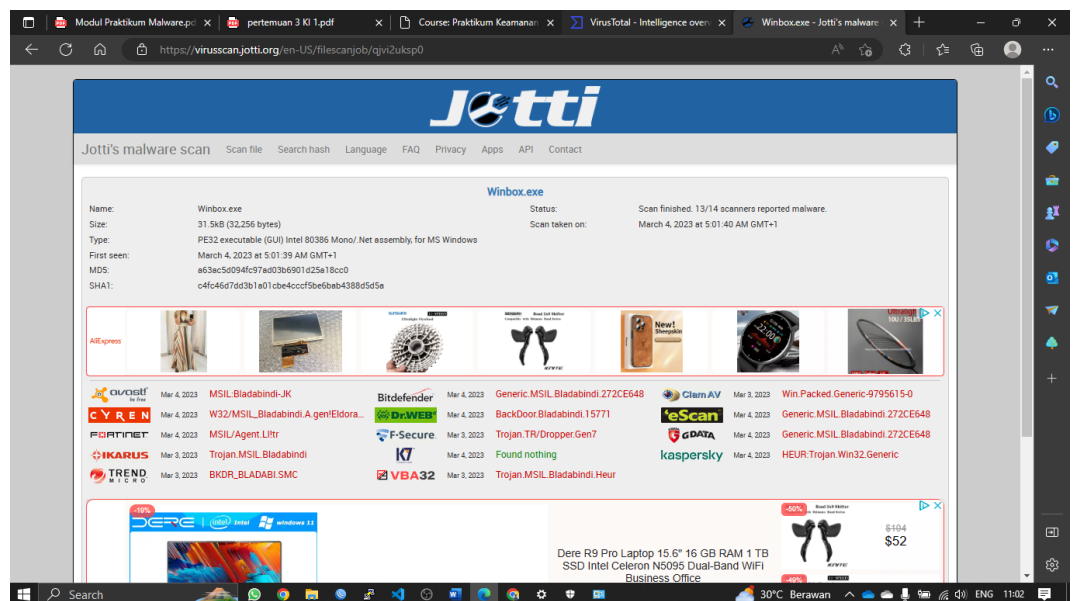
Network activities

Dynamic analysis detects ⓘ


31°C Sebagian cerah 12:52



d. Jotti



e. Polyswarm


POLYSWARM

[Scan](#)
[Search](#)
[Hunt](#)
[Engines](#)
[Pricing](#)
[Marketplace Stats](#)

[Log in / Sign up](#)

Summary

PolyScore™
0.99

15/18 Engines reported malicious

Winbox.exe


31.5 KB


PolyUnite family name


Bladabindi


SHA-256


e8746a18d4ced03d888
c6f4e7e70958e2fda08
744cab3fa0ca5e88039
c74ctdf


Rescan


Download


Share


Sandboxing


Privot

Detections

File Details

Network

Sandbox

JSON

Alibaba Bid: 0.0037	Gene.Win.Harmlet.157...	CiamAV 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	Virus.905885B191118E...	Ikarus Bid: 0.015	Trojan.MSIL.Bladabin...
NanoAV Bid: 0.015	Trojan.Win32.Gen8.ec...	Proton Bid: 0.015	Win.Dropper.njRAT
Qihoo 360 Bid: 0.015	HEUR/QVM03.0.B56F.Ma...	SecondWrite Bid: 0.015	
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 Bid: 0.0037	

27 engines not asserting

[English](#)
[Company Agreement](#)
[How It Works](#)
[Docs](#)
[Privacy Policy](#)
[Terms of Service](#)
[Engine](#)

2023 © PolySwarm Pte. Ltd.

VI. Kesimpulan

Pada praktikum kali ini dapat disimpulkan bahwa :

1.

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>

Klopmart. (February 23, 2021). 2 Kegunaan Solder, Komponen Beserta Jenis-Jenisnya. Retrieved August 21, 2022, from <https://www.klopmart.com/article/detail/kegunaan-solder>