

LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1

UNIT 4

ANALISIS MALWARE & NJRAT



Disusun oleh :

Nama : Aura Nisa' Hidayat
NIM : 21/482690/SV/19983
Kelas : TRI A
Dosen Pengampu : Anni Karimatul Fauziyyah, S.Kom., M.Eng.
Hari, Tanggal : Selasa, 28 Februari 2023

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

2023

Laporan Praktikum Kamanan Informasi 1

Unit 4: Analisis Malware & njRAT

I. TUJUAN

- Meneliti dan menganalisis malware

II. 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.

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 DAN BAHAN

- *Software* NJRAT
- Komputer atau laptop
- Akses internet

IV. TUGAS

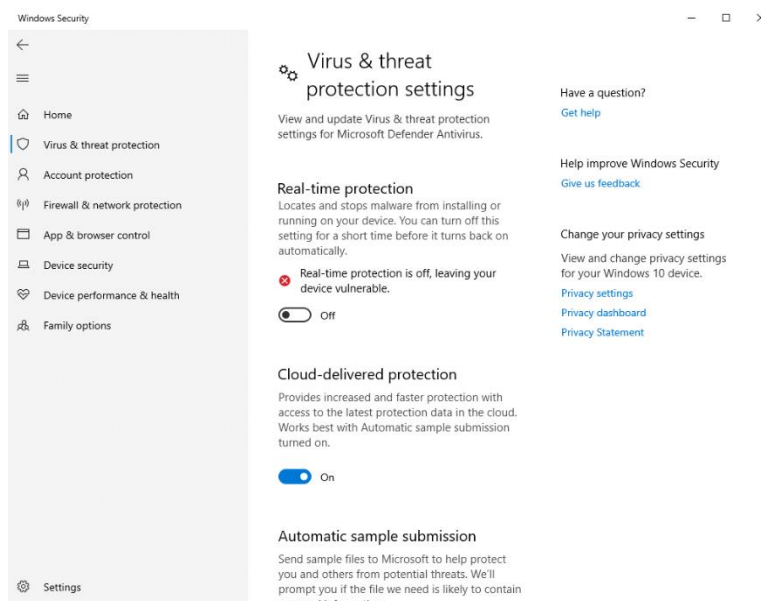
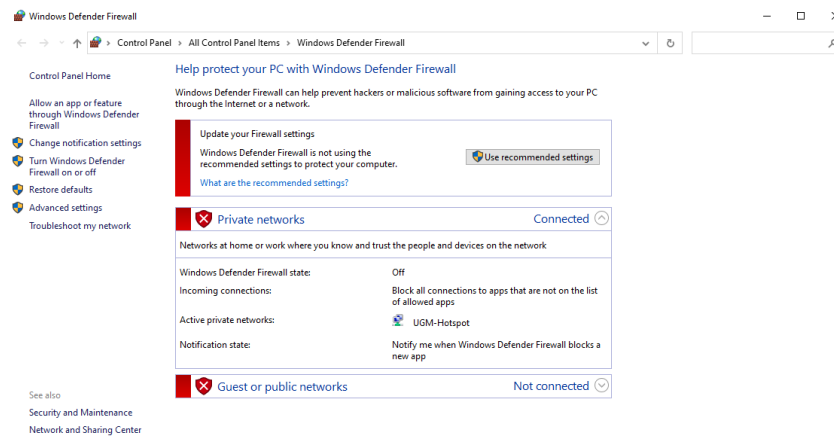
a. Analisis Anatomy Malware

1. Contoh jenis malware:

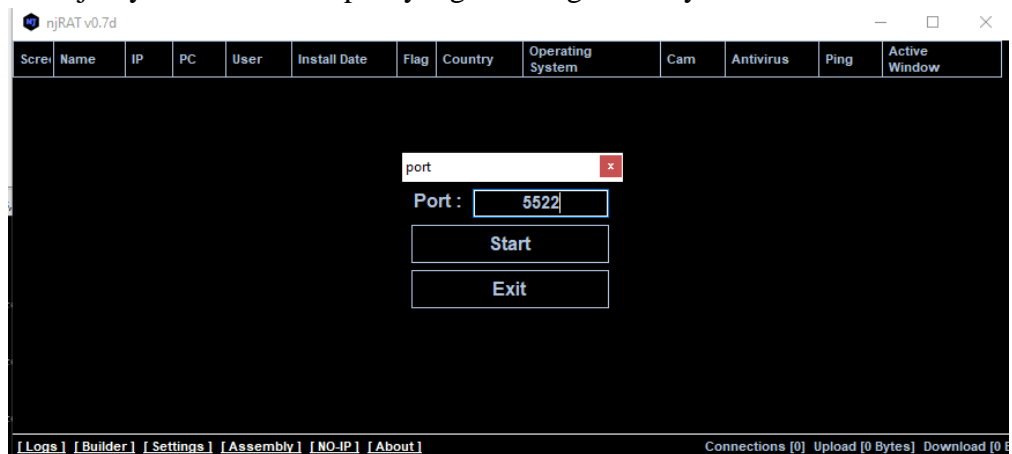
- Ransomware → malware jenis ini akan melakukan serangan dengan memblokir akses pengguna ke system komputer yang digunakan. Ransomware ditransmisikan dengan menggunakan trojan yang disamarkan menjadi file atau aplikasi, jika target membuka atau mendownload file tersebut, maka akan berdampak semua file pada perangkat komputer target akan terenkripsi.
- Trojan → jenis malware ini akan menyamar menjadi sebuah link, file, software, bahkan email yang seolah dari perusahaan resmi. Untuk mentransmisikan trojan membutuhkan bantuan korban, ketika target telah mengklik file yang dikirimkan, otomatis trojan akan aktif dan mengirimkan seluruh info dari device atau website. Trojan juga berdampak ke perangkat dan server yang terinfeksi, yaitu menularkan malware ke perangkat dan website yang saling terhubung.
- Exploit → exploit akan masuk ke komputer dan situs web untuk mencuri data. Ditransmisikan dengan menanamkan *malicious code* dalam sebuah situs web yang pada umumnya berupa iklan, jika diakses akan melakukan *redirect* ke halaman yang membuat pengguna mengunduh *exploit*. Malware ini akan menyerang aplikasi komputer target, dan dapat mengakses semua data pada komputer target.
- Adware → malware ini bertujuan untuk mendapatkan penghasilan dengan mengganggu pengguna dengan iklan yang ditampilkan pada *software* yang dipasang. Malware ini akan ditransmisikan ketika pengguna mengklik dan melihat iklan, hingga memasang aplikasi yang diminta. Adware memberikan dua dampak, yaitu baik dan buruk, dampak baiknya adalah memberikan opsi untuk tidak di-install dan menampilkan iklan yang tidak berpotensi mengganggu. Sedangkan dampak buruknya seringkali mengubah pengaturan browser dengan tujuan tampilan iklan yang lebih banyak, dan juga bisa ter-install sendiri tanpa izin dan tidak disadari pengguna.

b. Develop Malware Trojan dengan NJRAT

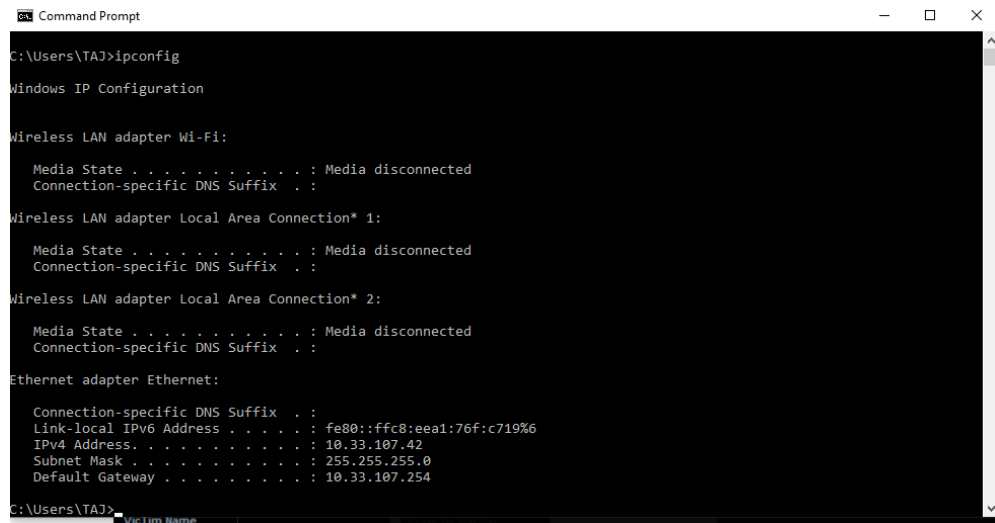
1. Langkah pertama adalah mematikan semua antivirus dan *firewall* pada kedua komputer yang akan digunakan untuk aplikasi NJRAT.



2. Kemudian *download* dan ekstrak aplikasi NJRAT, lalu jalankan aplikasi NJRAT pada komputer *host*.
3. Selanjutnya memasukkan port yang akan digunakan yaitu “5522”



4. Sebelumnya cek IP *address* milik komputer *host* terlebih dahulu melalui *commad prompt*. IP ini nantinya digunakan oleh NJRAT, pastikan juga komputer *victim* berada pada satu jaringan.



```
C:\Users\TAJ>ipconfig

Windows IP Configuration

Wireless LAN adapter Wi-Fi:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

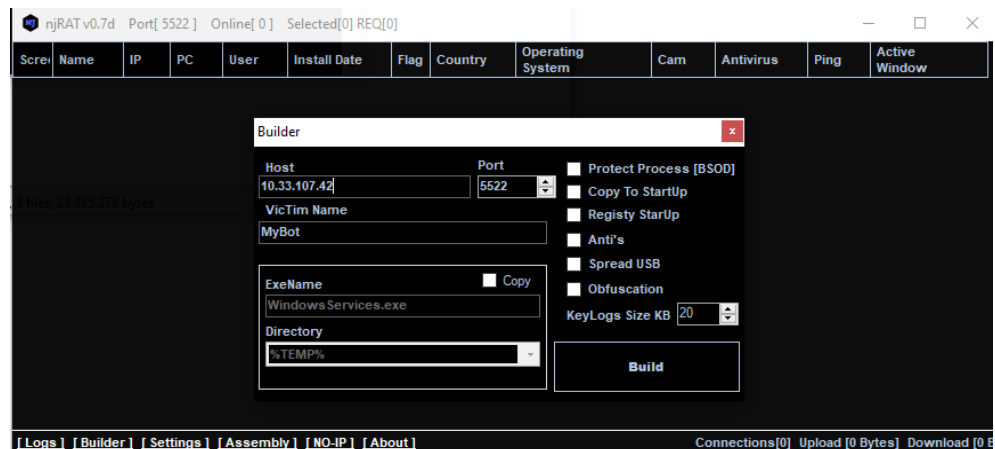
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet:

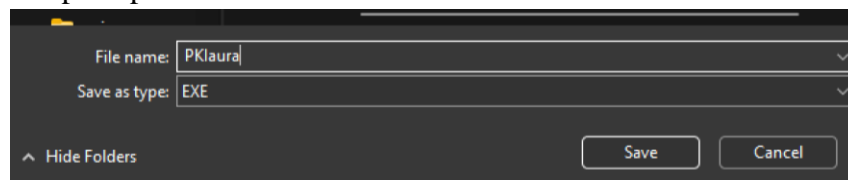
    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::ffc8:eea1:76f:c719%
    IPv4 Address. . . . . : 10.33.107.42
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.33.107.254

C:\Users\TAJ>
```

5. Lalu buat aplikasi yang akan dipasang pada komputer *victim* dengan memasukkan IP *address host* pada kolom *host* dan *port* yang sesuai dengan yang telah ditentukan sebelumnya agar dapat diakses oleh komputer, kemudian klik tombol *build*.

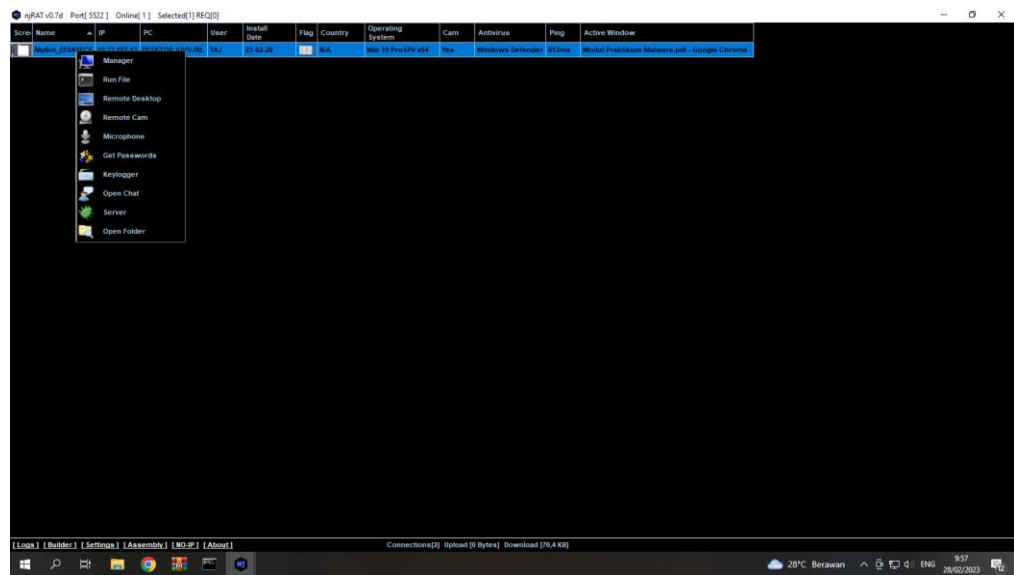


6. Simpan aplikasi hasil *build*.

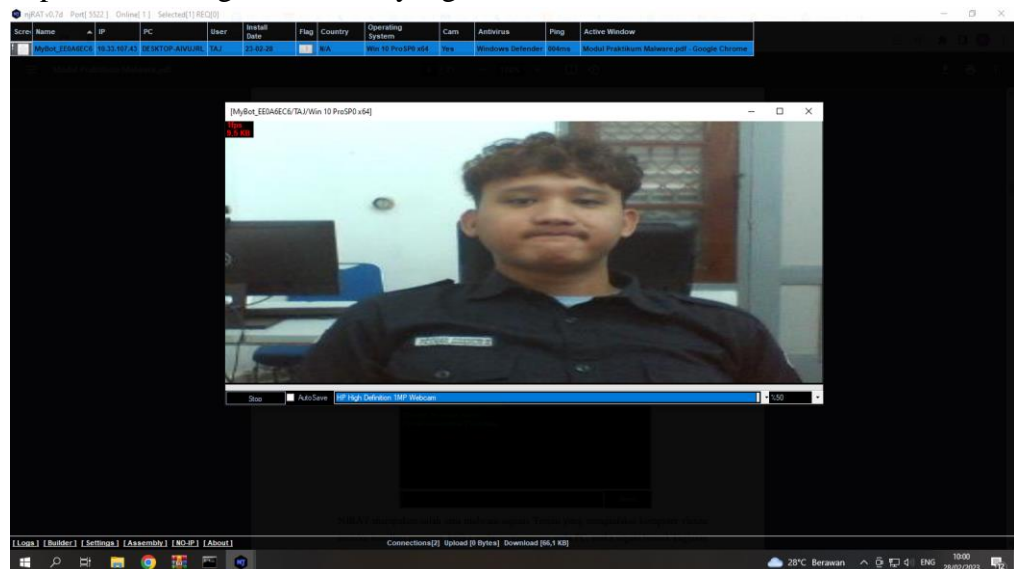


7. Kemudian *copy* hasil file *build* yang sudah dibuat ke dalam komputer *victim*, lalu jalankan pada komputer *victim*. NJRAT pada komputer *host* akan mendeteksi komputer *victim*.

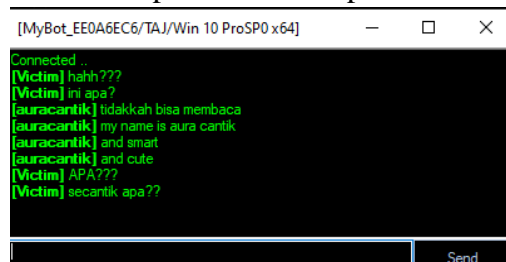
8. Klik kanan pada komputer yang aktif maka akan terdapat beberapa pilihan menu.



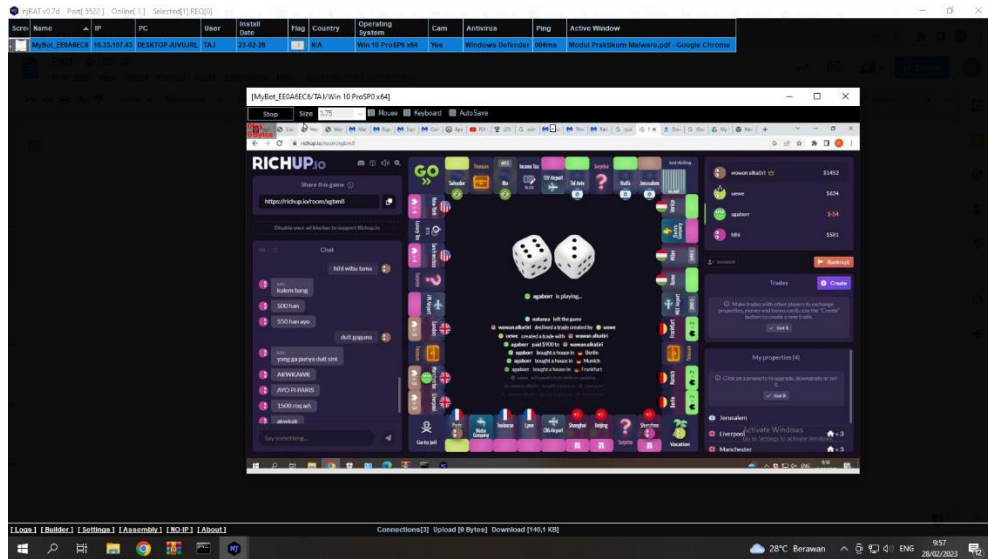
9. Pilih salah satu menu untuk mencoba, berikut yang pertama adalah menu *remote cam* dan otomatis akan membuka *webcam* yang ada pada komputer *victim* lalu dapat melihat segala aktivitas yang dilakukan oleh *victim*.



10. Yang kedua mencoba menu *chat message*, dengan ini kita dapat mengirimkan pesan ke layer *desktop* komputer *victim*, dan user komputer dapat melakukan balasan tanpa bisa menutup chat.

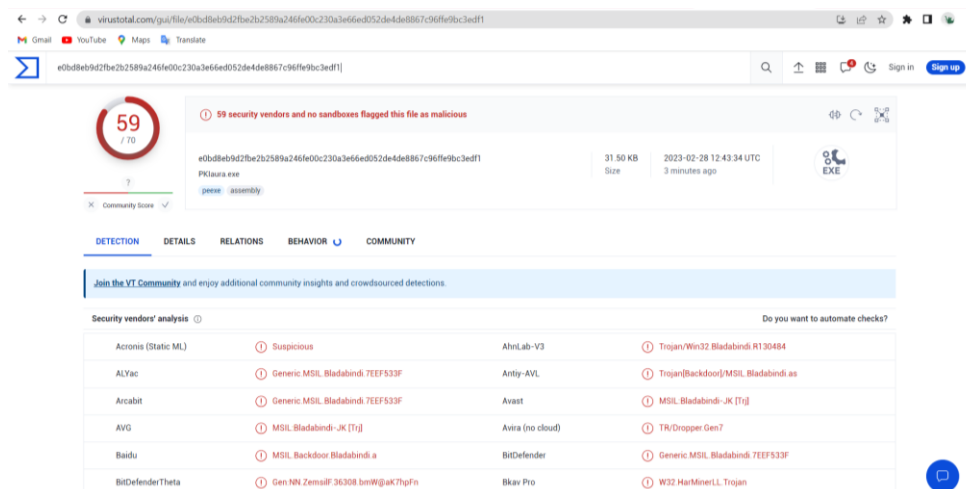
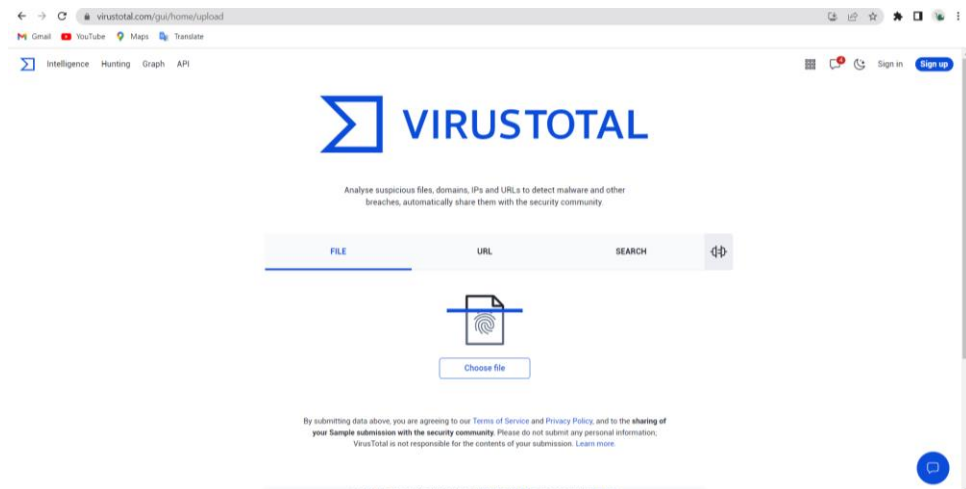


11. Ketiga mencoba menu *remote desktop*.

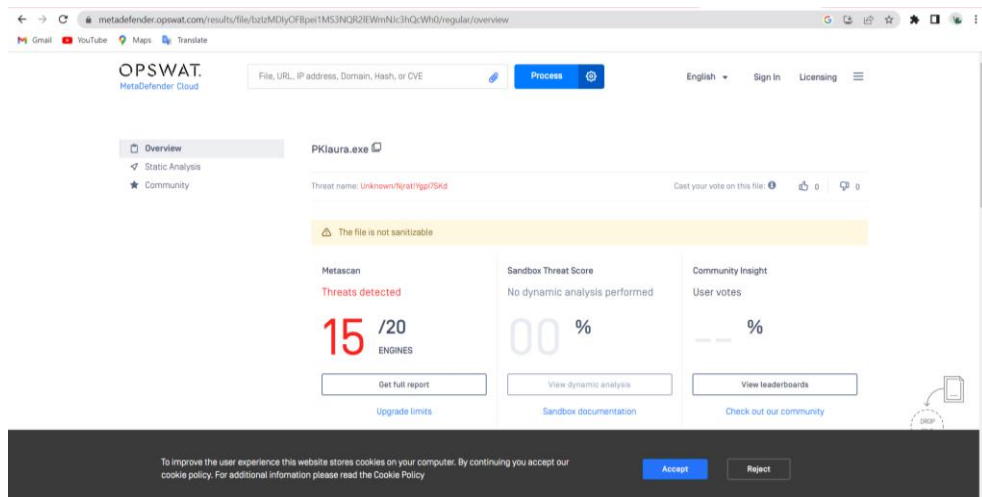
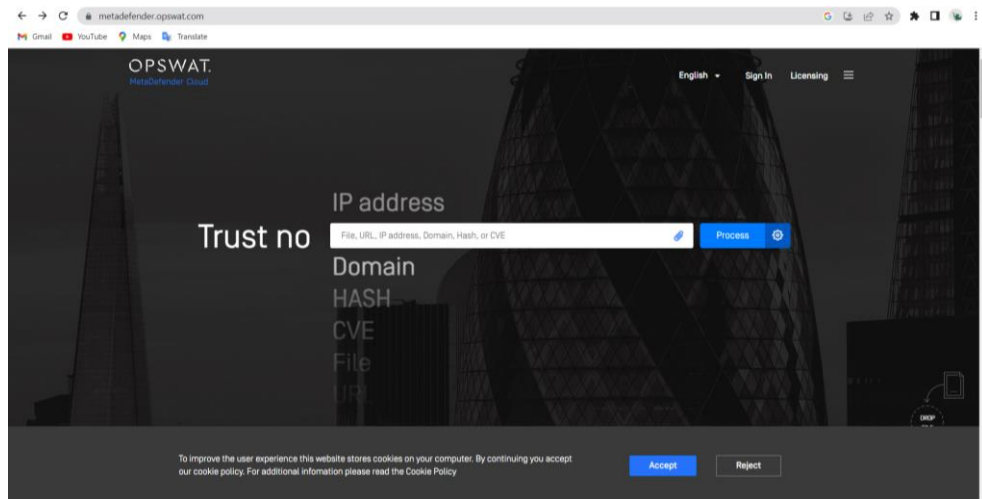


c. Analisis Malware dengan Metode OSINT

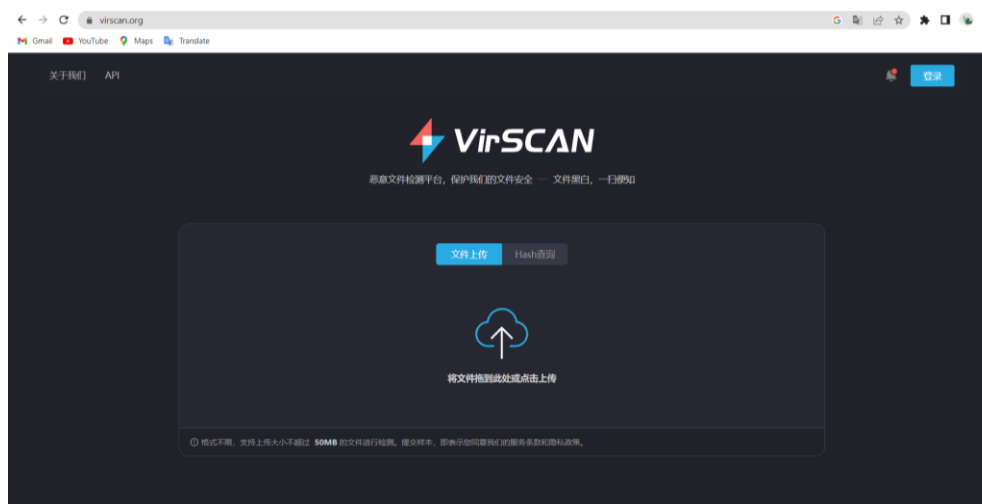
1. VirusTotal



2. OPSWAT Meta Defender



3. VirSCAN



virscan.org/report/v0b8dbef942fba2b2589a246a00c230a3e6ed052de4de0867c96ffefbc3edf1

VirSCAN 请输入Hash值 (MD5, SHA1, MD5)

PKIaura.exe 19/27 引擎检出

SHA256: e0b8dbef942fba2b2589a246a00c230a3e6ed052de4de0867c96ffefbc3edf1
 SHA1: 5e3ae99f74ea1e643c6f28ba6e533f1e6d53fe
 MD5: 48b9d29c65d63d6d9f6aa7b36599

文件大小: 31.5 KB (32256)
 文件类型: pe
 首次提交: 2023/02/28 19:54:25 (GMT+7)
 再次分析: 2023/02/28 19:55:00 (GMT+7)

引擎检测 静态信息

本次检测时间: 2023-02-28 19:55:00

引擎	结果	引擎	结果
AVG	MSIL.Bladabindi-JK	Authentium	W32/MIL_Bladabindi.Agent.Iborado
Antiy	Trojan.Backdoor.MSIL.Bladabindi.an	Comodo	Backdoor.MSIL.Bladabindi.BA@Trojan
Arcabit	Generic.MSIL.Bladabindi.7EEF533F	JiangMin	Trojan.Dropper.AutoIt.dce
OneAV	Win.Malicious.mf	F-Prot	W32/MIL_Bladabindi.A2.gen@Iborado
Avira	TR/Dropper.Gen7	Avast	MSIL.Bladabindi-JK
Cyren	W32/MIL_Bladabindi.Agent.Iborado	VBA32	Trojan.MSIL_Bladabindi.Heur

4. Jotti

virusscan.jotti.org

Jotti's malware scan

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

About Jotti's malware scan

Jotti's malware scan is a free service that lets you scan suspicious files with several anti-virus programs. You can submit up to 5 files at the same time. There is a 250MB limit per file. Please be aware that no security solution offers 100% protection, not even when it uses several anti-virus engines. All files are shared with anti-virus companies so detection accuracy of their anti-virus products can be improved.

Submit files

Browse...

Scanners used

Avast, Avira, BitDefender, ClamAV, Comodo, Cyren, Emsisoft, F-Secure, GData, Ikarus, Kaspersky, McAfee, Nod32, Norton, Panda, QuickHeal, Symantec, Trend Micro, VirusBolt, VBA32, Webroot, Yandex, Zillya, ZN

© 2004-2023 Jotti

Jotti's malware scan

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

PKIaura.exe

Name: PKIaura.exe
 Size: 31 KB (32,256 bytes)
 Type: PE32 executable (GUI) Intel 80386 Mono/Net assembly for MS Windows
 First seen: February 28, 2023 at 1:57:58 PM GMT+1
 MD5: 48b9d29c65d63d6d9f6aa7b36599
 SHA1: 5e3ae99f74ea1e643c6f28ba6e533f1e6d53fe

Status: Scan finished: 13/14 scanners reported malware
 Scan taken on: February 28, 2023 at 1:57:59 PM GMT+1

Cyren	Feb 28, 2023	MSIL.Bladabindi-JK	BitDefender	Feb 28, 2023	Generic:MSIL.Bladabindi.7EEF533F	ClamAV	Feb 28, 2023	Win.Packed.Generic/5795615-0
Cyren	Feb 28, 2023	W32/MIL_Bladabindi.Agent.Iborado	BitDefender	Feb 28, 2023	Backdoor.Bladabindi.15771	ClamAV	Feb 28, 2023	Generic:MSIL.Bladabindi.7EEF533F
Fortinet	Feb 28, 2023	MSIL/Agent.Lfr	BitDefender	Feb 28, 2023	Trojan.Tro/Dropper.Gen7	ClamAV	Feb 28, 2023	MSIL.Trojan.Spy.Bladabindi.BQ
Ikarus	Feb 28, 2023	Trojan.MSIL.Bladabindi	BitDefender	Feb 28, 2023	Found nothing	ClamAV	Feb 28, 2023	HEUR.Trojan.Win32.Generic
Trend Micro	Feb 27, 2023	EXOR.BLADABINDI.SMC	BitDefender	Feb 28, 2023	Trojan.MSIL.Bladabindi.Heur	ClamAV	Feb 28, 2023	

© 2004-2023 Jotti

5. BitBaan MaLab

multibitbitbaan.com/en/home

Home Lang Login

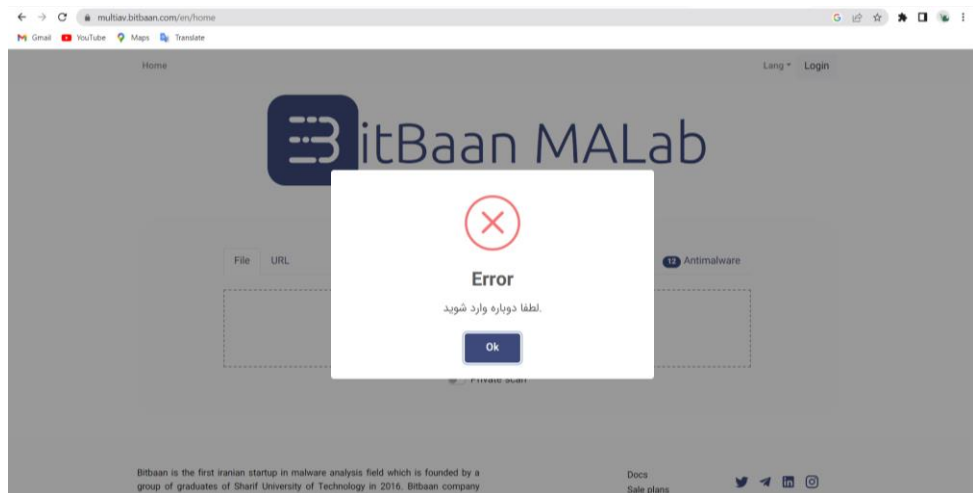
BitBaan MALab

File URL

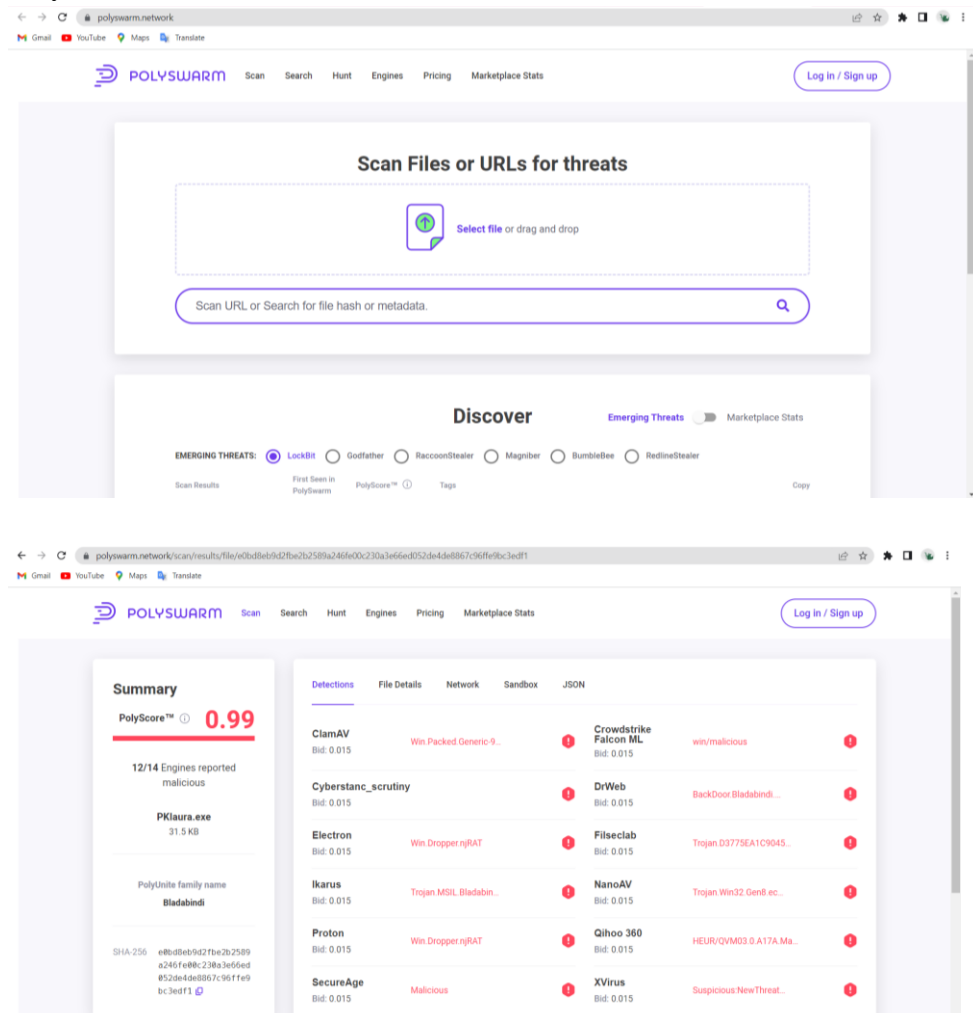
Antimalware

To select your file, Click or Drop

Private scan



6. PolySwarm



V. PEMBAHASAN

a. Analisis Anatomy Malware

Malware merupakan perangkat lunak yang bekerja dengan memasuki komputer tanpa perizinan serta dapat menyebabkan kerusakan pada system, server, dan jaringan komputer. Terdapat banyak jenis malware yang perlu kita waspadai, yang pertama ada virus yang bisa didapatkan melalui unduhan pada situs web, penggunaan USB, dokumen komputer, koneksi jaringan, dan lain sebagainya. Kemudian terdapat Adware yang dapat masuk ke jaringan komputer dan mengaksesnya melalui iklan pada situs web. Berikutnya adalah Trojan yang bekerja dengan melakukan penyamaran sebagai sebuah aplikasi yang tidak berbahaya sehingga meyakinkan pengguna untuk mengunduh dan menggunakan aplikasi tersebut. Selanjutnya yaitu Ransomware yang bekerja dengan cara mengunci dan menolak pengguna untuk akses data komputer, pada umumnya jenis ini digunakan oleh hacker untuk kejahatan cyber dan meminta sejumlah uang sebagai tebusan.

Dampak serangan Malware dapat merusak data dan dokumen, memperlambat sistem komputer, mendapatkan kendala pada aplikasi di dalamnya, hingga perubahan data menjadi virus. Hal ini dapat diatasi dengan rutin melakukan pemindaian dan melakukan pencadangan. Melakukan Analisa malware dengan metode OSINT, dengan menggunakan salah satu dari sekian banyak *platform* yang dapat digunakan untuk memindai data.

b. Develop Malware Trojan dengan NJRAT

Develop malware trojan dengan *software* NJRAT atau *Remote Administrator Tool* yang digunakan untuk membuat file dengan tujuan mendapatkan akses ke sistem pengguna. Trojan sendiri merupakan sebuah malware yang dapat digunakan untuk mendapatkan hak akses sistem pengguna. Kemudian NJRAT dapat menghubungkan dan mengatur satu komputer atau lebih dengan berbagai kemampuan yaitu, *remote desktop*, *remote cam*, *chat*, akses file, mengontrol komputer, akses password, dan lain sebagainya. Singkatnya NJRAT merupakan salah satu Malware sejenis Trojan yang dapat menginfeksi komputer *victim* melalui *installasi* program. Pada praktikum kali ini saya mencoba menu *remote cam*, *open chat*, dan *remote desktop*. Yang pertama adalah menu ***remote cam*** yang mana menu ini akan otomatis membuka *webcam* yang ada pada komputer *victim* lalu dapat melihat segala aktivitas yang dilakukan oleh *victim*. Selanjutnya ***open chat*** dengan ini kita dapat mengirimkan pesan ke layer *desktop* komputer *victim*, dan user komputer dapat melakukan balasan tanpa bisa menutup chat. Dan terakhir mencoba menu ***remote desktop***, dengan fitur ini kita dapat mengendalikan segala aktivitas pada komputer *victim* melalui komputer *host*.

d. Analisis Malware dengan Metode OSINT

Analisis Malware dengan metode OSINT atau *Open Source Intelligent* merupakan suatu metode untuk mengumpulkan, menganalisis, serta membuat suatu keputusan terkait data yang dapat diakses di ruang publik. Pada bidang *cyber security* juga menggunakan metode OSINT untuk mengumpulkan data-data yang

dibutuhkan seperti mengidentifikasi perentas. Yang pertama yaitu **VirusTotal** yang merupakan salah satu *platform online* gratis untuk menganalisisi berkas dan pranala (URL) dari virus, worm, trojan, dan segala jenis perangkat perusak dengan menggunakan 54 mesin antivirus. Dari hasil pemindaian yang dilakukan pada file NJRAT yang digunakan sebelumnya menunjukkan bahwa hanya dapat dideteksi dengan 11 *security vendor*, 59 dari 70 *security vendor* tidak menandai jika file tersebut berbahaya. Selanjutnya **OPSWAT** yang merupakan salah satu produk *cyber security*, menunjukkan bahwa 15 dari 20 bagian file NJRAT terdeteksi berbahaya. Kemudian deteksi menggunakan **VirSCAN** menunjukkan hasil 27 dari 46 bagian file NJRAT terdeteksi berbahaya. Lalu menggunakan **Jotti** menggunakan 13 *scanner* dari 14 *scanner* yang dapat menandakan file NJRAT berbahaya. Selanjutnya pada *platform Bitbaan* **MALab** terjadi eror saat *upload file*. Terakhir adalah **PolySwarm** yang merupakan perusahaan keamanan siber yang membantu pengguna, perusahaan, dan tim keamanan perusahaan mendeteksi dan mengumpulkan intelijen tentang malware baru dan yang sedang berkembang. Dari hasil *scan* terdapat 12 dari 14 mesin berbahaya.

VI. KESIMPULAN

Dari praktikum keamanan informasi kali ini dapat disimpulkan bahwa:

1. Malware atau perangkat lunak berbahaya dapat digunakan untuk menyebabkan kerusakan pada sistem komputer, mencuri data, dan melewati tindakan keamanan.
2. Malware dapat diatasi dengan melakukan pemindaian dan melakukan pencadangan.
3. Terdapat banyak jenis malware yang dapat merusak system komputer.
4. njRAT salah satu jenis malware Trojan yang digunakan untuk mendapatkan hak akses sistem pengguna.
5. njRAT adalah salah satu tools hacking untuk OS windows.
6. RAT adalah singkatan dari *Remote Administrator Tool* yang di gunakan untuk menghubungkan dan mengatur satu atau lebih komputer.
7. Metode OSINT (*Open Source Intelligent*) merupakan suatu metode untuk mengumpulkan, menganalisis, serta membuat suatu keputusan terkait data yang dapat diakses di ruang publik.

DAFTAR PUSTAKA

- Apa Itu OSINT (Open Source Intelligence)?* (2020, November 23). Retrieved Maret 5, 2023, from Monitor Teknologi: <https://www.monitorteknologi.com/apa-itu-osint/>
- Benefita. (2021, Juni 28). *Ketahui Cara Kerja Trojan dan Cara Mengatasinya*. Retrieved Maret 5, 2023, from NiagaHoster Blog: <https://www.niagahoster.co.id/blog/cara-kerja-trojan/>
- Bersama, I. (2020, Februari 24). *Malware - njRAT (Remote Access Trojan)*. Retrieved Maret 4, 2023, from IlmuBersama.com: <https://ilmubersama.com/2020/02/24/malware-njrat-remote-access-trojan/>
- Citra, N. (n.d.). *Cara Menggunakan NJRAT (Trojan)*. Retrieved Maret 4, 2023, from Network Security: <http://nabillahcitra.blogspot.com/2016/12/cara-menggunakan-njrat-trojan.html>
- Hikmawati, A. (2020, Agustus 17). *Bagaimana Cara Kerja Ransomware? - Memahami Cara Kerja Ransomware Yang Dapat Menyerang Sistem IT Perusahaan*. Retrieved Maret 5, 2023, from Zettagrid: <https://www.zettagrid.id/blog/2020/08/17/cara-kerja-ransomware/>
- Kirova, D. (2022, Januari 14). *Tempat membeli PolySwarm, token perusahaan keamanan siber yang populer*. Retrieved Maret 5, 2023, from CoinJournal: <https://coinjournal.net/id/berita/tempat-membeli-polyswarm-token-perusahaan-keamanan-siber-yang-populer/>
- Pengertian Malware serta Jenis dan Cara Mengatasinya Dengan Tepat*. (2022, Juli 15). Retrieved Maret 5, 2023, from Cloud Matika: <https://www.cloudmatika.co.id/blog-detail/apa-itu-malware#:~:text=Trojan%20merupakan%20malware%20yang%20bekerja,dan%20melihat%20seluruh%20aktivitas%20komputer.>
- Rabbani, A. (n.d.). *Adware: Pengertian, Penyebab, Cara Kerja, Jenis, Contoh, Dampak, dan Cara Mengatasinya*. Retrieved Maret 5, 2023, from Sosial79: <https://www.sosial79.com/2022/06/adware-pengertian-penyebab-cara-kerja.html>
- Sistemas, H. (2004, Juni). *VirusTotal*. Retrieved Maret 5, 2023, from TopLoker.com: <https://p2k.stekom.ac.id/ensiklopedia/VirusTotal>
- TIK, U. (2017, September 4). *Mengenal Ransomware dan Pencegahannya*. Retrieved Maret 5, 2023, from UPTTIK: <https://upttik.undiksha.ac.id/mengenal-ransomware-dan-pencegahannya/>