

**LAPORAN PRAKTIKUM  
PRAKTIKUM KEAMANAN INFORMASI 1  
UNIT 3  
ANALISIS ANATOMI MALWARE & NJRAT**



**DI SUSUN OLEH**

Nama : Prama Yugas Nurhakim  
NIM : 21/474280/SV/18892  
Hari, Tanggal : Selasa, 28 Februari 2023  
Kelas : A

**SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET  
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA  
SEKOLAH VOKASI  
UNIVERSITAS GADJAH MADA  
YOGYAKARTA  
2023**

## **A. Tujuan**

1. Mengeksplorasi njRAT
2. Melakukan Serangan Malware Njrat Pada PC

## **B. Latar Belakang**

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 di upload ke tidak menganggapnya sebagai sebuah trojan. [virustotal.com](https://www.virustotal.com) , hanya 4 antivirus yang 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 !!

## C. Alat dan Bahan

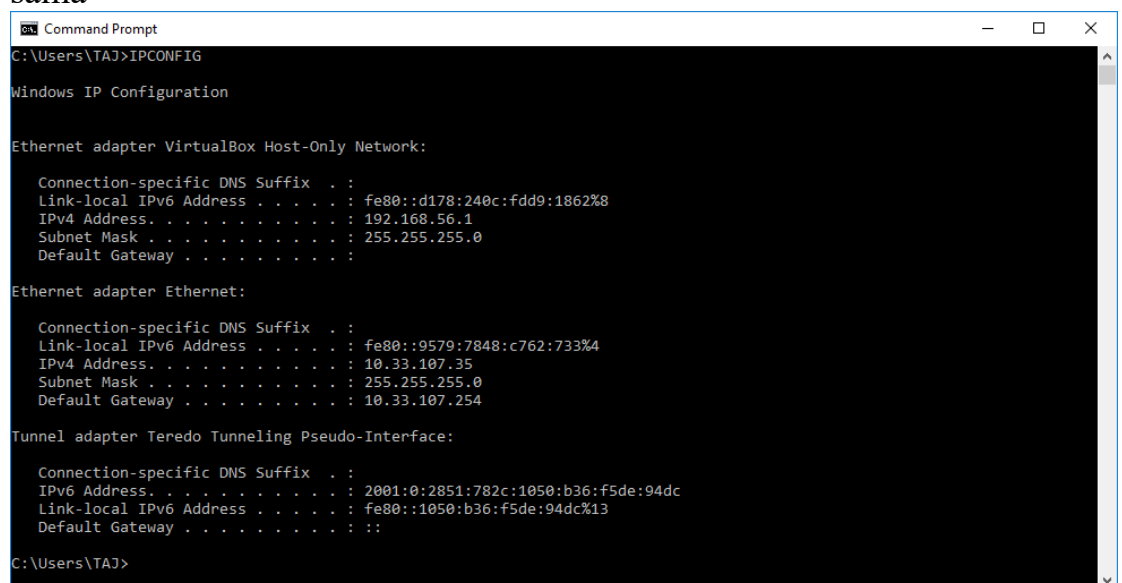
- 1) njRAT software
- 2) Koneksi Internet

## D. Instruksi Kerja

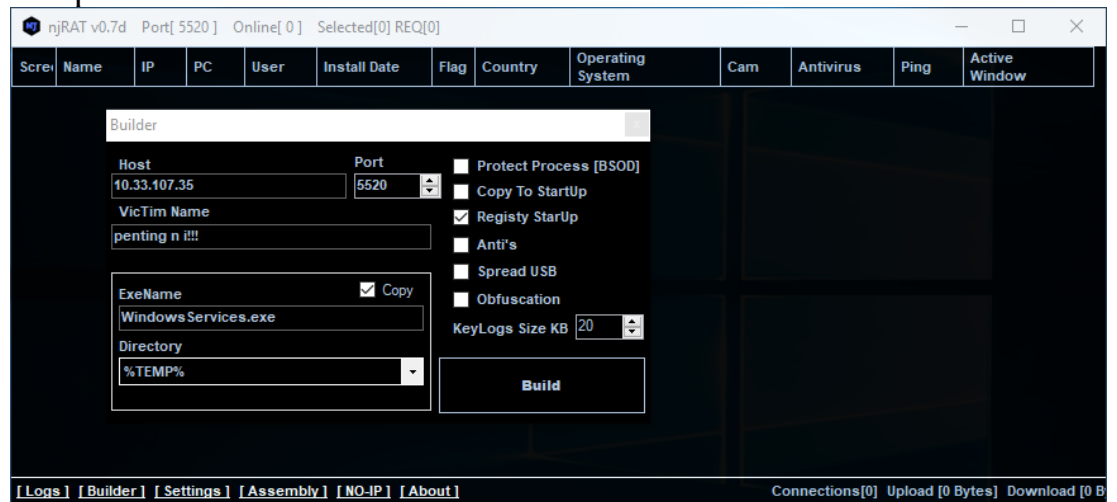
1. Pada software njRAT isikan port 5520 dan start



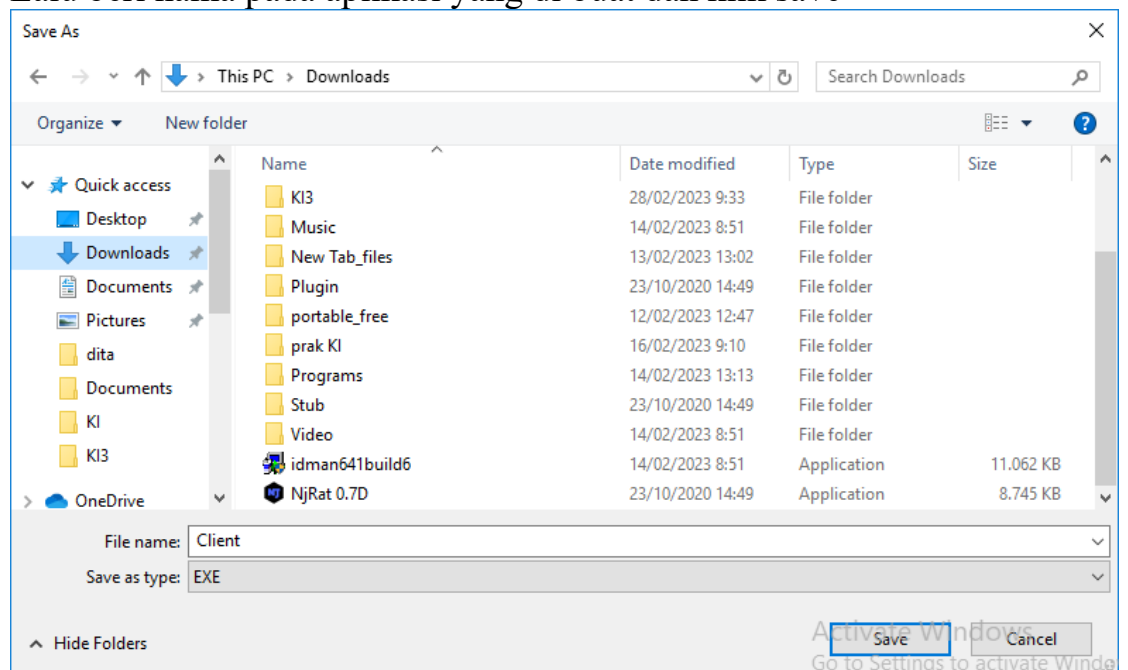
2. Selanjutnya cek ip address host, IP ini dipakai pada njRAT dan pastikan juga computer victim juga berada pada satu jaringan yang sama



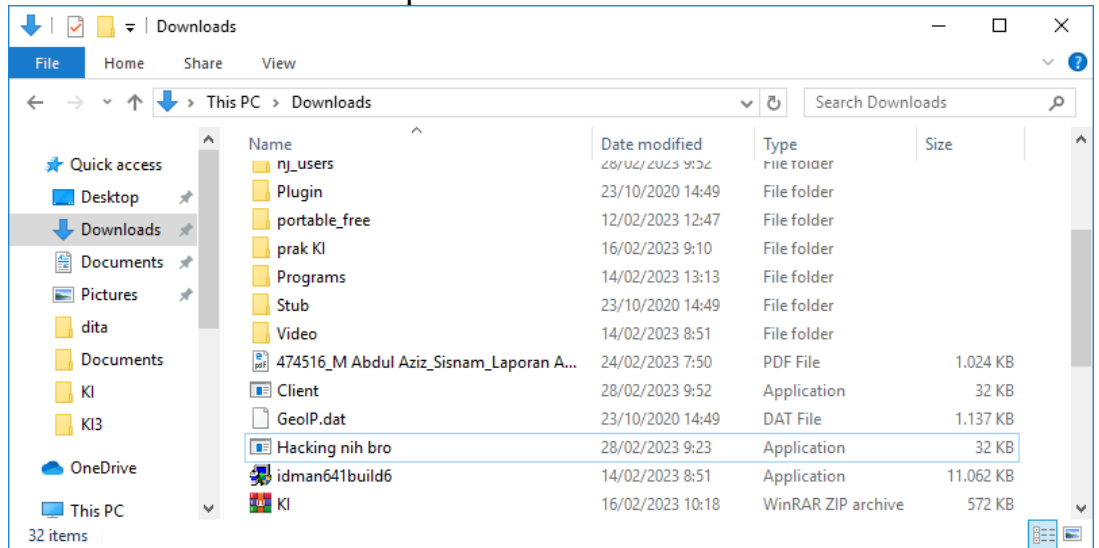
3. Yang Buat aplikasi yang akan dipasang pada komputer victim. Masukkan IP Address host pada kolom host dan port yang sesuai dengan yang sesuai pada aplikasi njRAT agar dapat di akses oleh computer nanti dan klik tombol build.



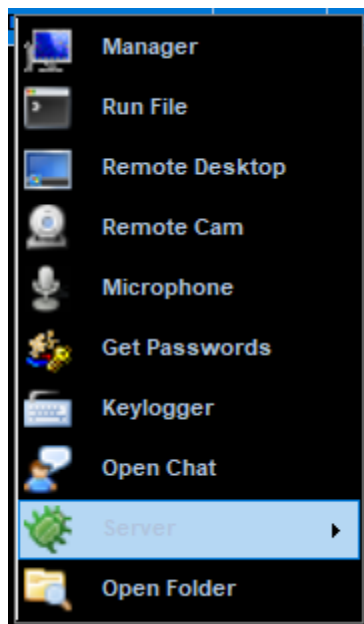
4. Lalu beri nama pada aplikasi yang di buat dan klik save



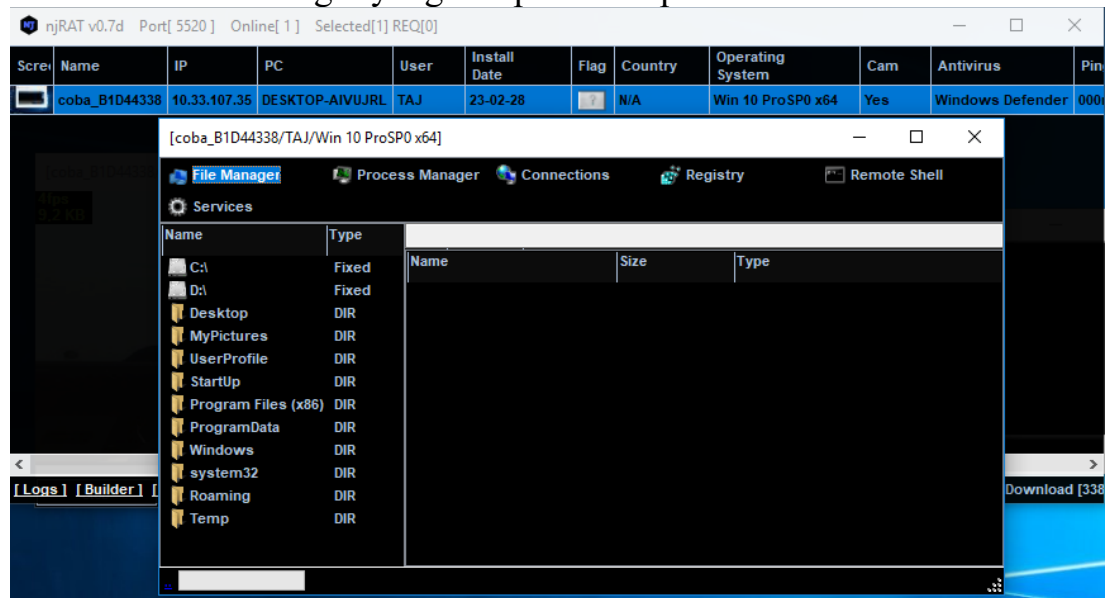
5. Lalu salin dan masukkan aplikasi kedalam computer victim dan jalankan aplikasi tersebut dengan cara klik 2 kali maka NJRAT pada host akan mendeteksi komputer victim



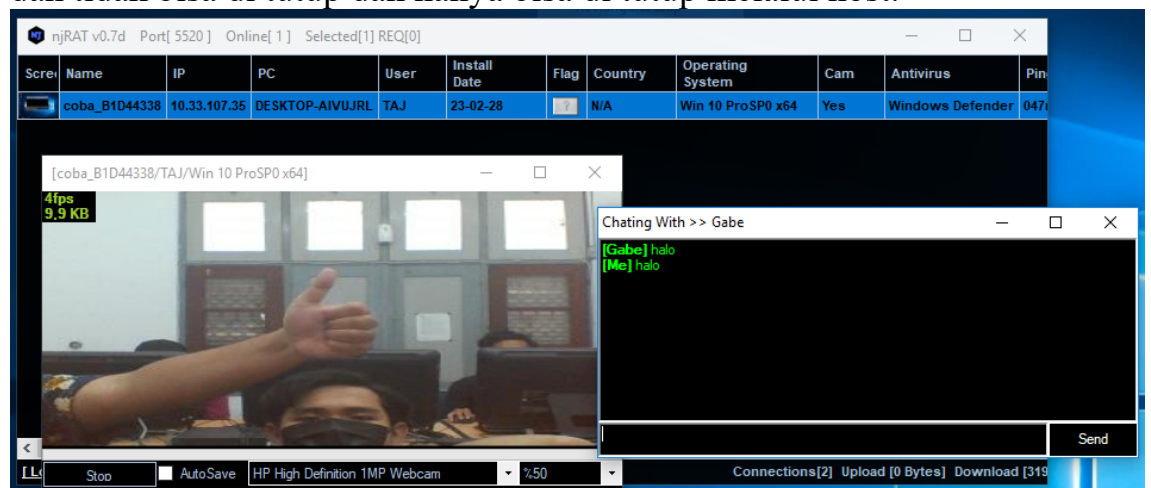
6. Buka njRAT lalu klik kanan dan akan muncul fungsi fungsi yang bisa dilakukan host untuk mengatur pada computer victim



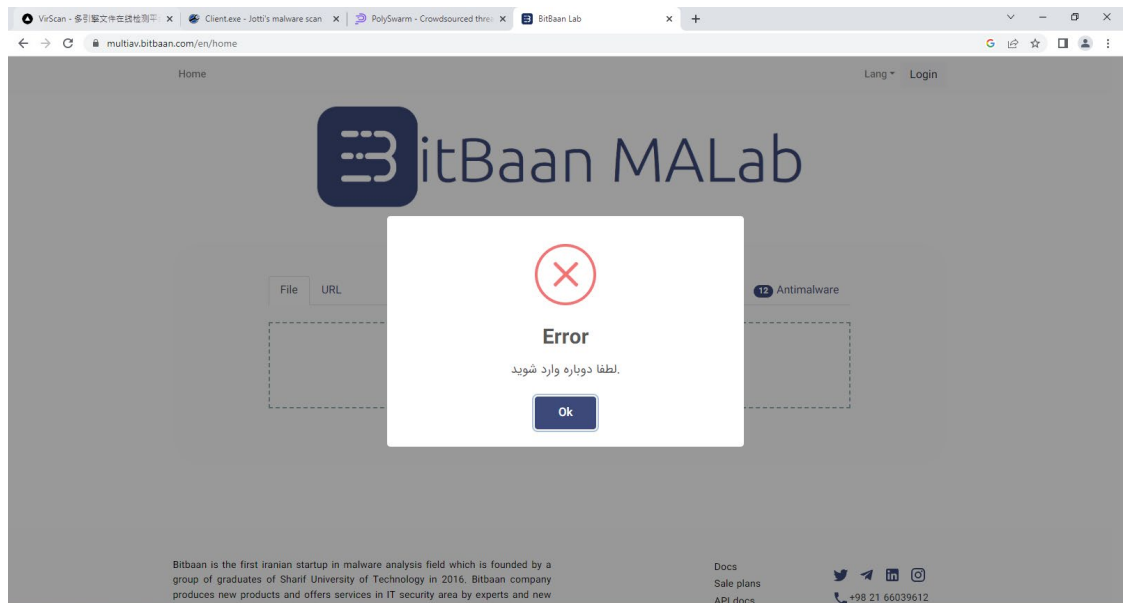
7. Tampilan jika memilih fungsi manager maka akan bisa melihat seluruh isi file manager yang ada pada komputer victim



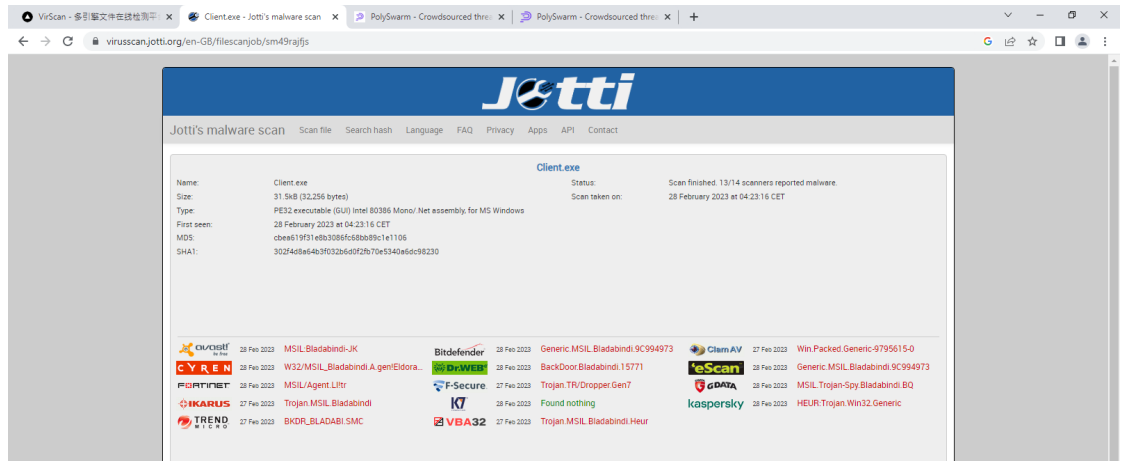
8. Lalu jika memilih fungsi remote cam akan membuka webcam milik victim secara paksa, dan open chat akan muncul pop up di victim dan tidak bisa di tutup dan hanya bisa di tutup melalui host.



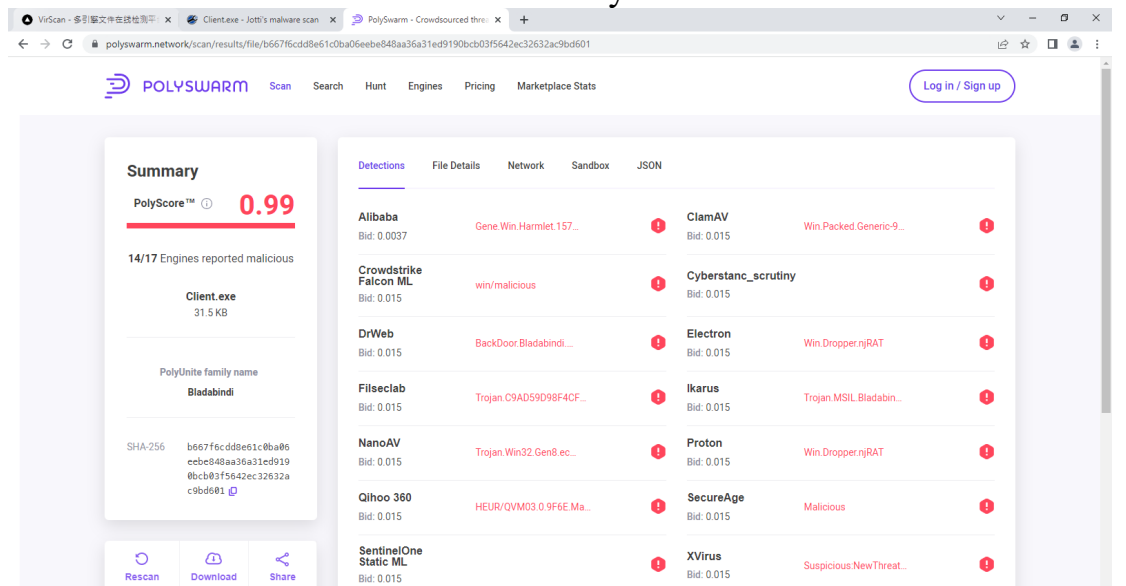
## 9. Scan metode Osint analisis malware Bitbaan MALab



## 10. Scan metode Osint analisis malware Jotti



## 11. Scan metode Osint analisis malware Polyswarm



## 12.Scan metode Osint analisis malware VirSCAN

VirScan - 多引擎文件在线扫描平台 | Client.exe - Jotti's malware scan | PolySwarm - Crowdsourced threat analysis | PolySwarm - Crowdsourced threat analysis

virscan.org/report/b667f6cdd8e61c0ba05eebe848aa36a31ed9190bcb03f5642ec32632ac9bd601

VirSCAN 请输入Hash值 (支持SHA256, SHA1, MD5)

**Client.exe** 有 25 引擎检出

SHA256: b667f6cdd8e61c0ba05eebe848aa36a31ed9190bcb03f5642ec32632ac9bd601 文件大小: 31.5 KB (32256)  
SHA1: 302f4d8a64b3f0326d0f2b70e5340a6dc98230 文件类型: pe  
MD5: cbee619f31e8b3086fc68bb89c1e1106 首次提交: 2023/02/28 10:22:21 (GMT+7)  
再次分析: 2023/02/28 10:23:43 (GMT+7)

引擎检测 静态信息

再次检测时间: 2023-02-28 10:23:43

引擎	结果	引擎	结果
AVG	MSIL:Bladabindi.JK	Authenticam	W32/MSIL_Bladabindi.AgenEldorado
Cyren	W32/MSIL_Bladabindi.AgenEldorado	F.Prot	W32/MSIL_Bladabindi.A2.genEldorado
VBA32	Trojan.MSIL.Bladabindi.Heur	Avira	TR/Dropper.Gen7
Fortinet	MSIL/Agent.Littr	IKARUS	Trojan.MSIL.Bladabindi
McAfee	BackDoor-NJratCBEA619F31E8	Dr.Web	BackDoor.Bladabindi.15771
ClamAV	Win.Packed.Generic-9795615-0	Antiy	Trojan(Backdoor)/MSIL.Bladabindi.Las
Comodo	Backdoor.MSIL.Bladabindi.BA@7cej5x	Arcabit	Generic.MSIL.Bladabindi.9C994973

## 13.Scan metode Osint analisis malware OPSWAT. MetaDefender Cloud

OPSWAT. MetaDefender Cloud

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

Process

English Sign In Licensing

Overview

Static Analysis

Multiscanning 12

PE Information

Scan History 1

Community

file.exe

Threat name: Trojan/Njrat/DTDZ/Ncp

Cast your vote on this file: 0 0

Metascan Multiscan

Threats detected

12 /16 ENGINES

Multiscanning, is an advanced threat detection and prevention technology that increases detection rates, decreases outbreak detection times and provides resiliency to anti-malware vendor issues.

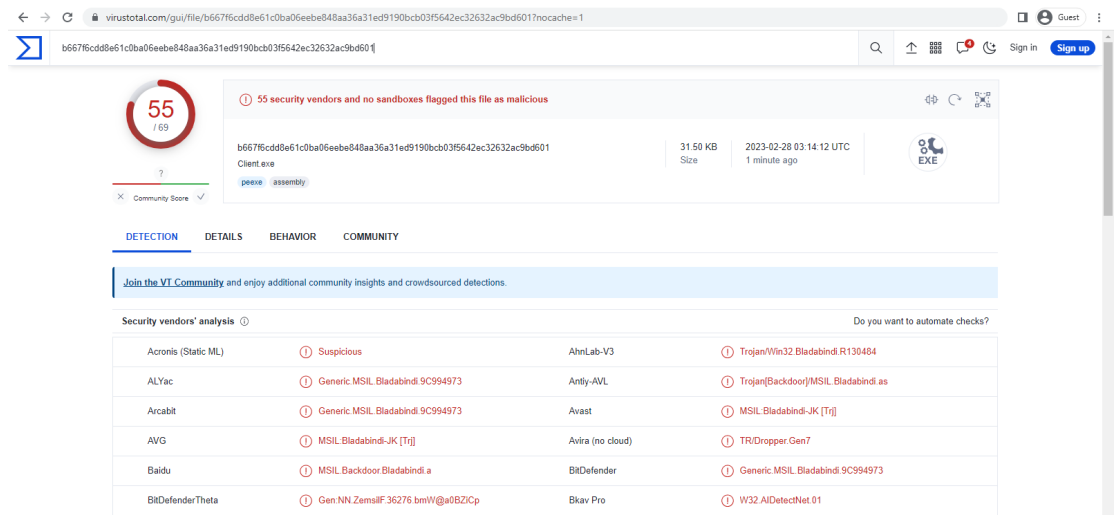
OPSWAT pioneered the concept of multi-scanning files with over 30 anti-malware engines available to deliver enhanced protection from a variety of cyber threats.

[Learn more about Multiscanning.](#)

Result	Engine	Last Update
✗ Win.Packed.Generic-9795615-0	ClamAV	Feb 27, 2023
✗ Trojan.MSIL.Bladabindi	IKARUS	Feb 27, 2023
✗ TR/Dropper.Gen7	Avira	Feb 27, 2023
✗ Trojan.Win32.Generic.LA1H	AegisLab	Feb 26, 2023
✗ Backdoor/W32.DN-NJrat.32256	TACHYON	Feb 27, 2023
✗ Confidence_96	RocketCyber	Feb 27, 2023
✗ Trojan.Bladabindi.Win32.99364	Zillya!	Feb 25, 2023
✗ Trojan (700000121)	K7	Feb 27, 2023
✗ Generic.MSIL.Bladabindi.5680F27F	Bitdefender	Feb 27, 2023
✗ Win/Malicious_confidence_100	CrowdStrike Falcon ML	Feb 27, 2023
✗ Trojan/Win32.Bladabindi	AhnLab	Feb 28, 2023
✗ ML: Suspicious	Vir.IT ML	Feb 24, 2023
⚠ Suspicious	Filescab	Feb 27, 2023
✓ No Threat Detected	Xvirus Anti-Malware	Feb 27, 2023
✓ No Threat Detected	Quick Heal	Feb 27, 2023
⚠ Unsupported File Type	QnAV	Feb 27, 2023



## 14. Scan metode Osint analisis malware Virustotal



55 / 69

55 security vendors and no sandboxes flagged this file as malicious

b667f6cdd8e61c0ba06eebe848aa36a31ed9190bcb03f5642ec32632ac9bd601

31.50 KB Size

2023-02-28 03:14:12 UTC 1 minute ago

Client.exe

peexe assembly

Community Score

DETECTION DETAILS BEHAVIOR COMMUNITY

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

Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan.Win32.Bladabindi.R130484
ALYac	Generic.MSIL.Bladabindi.9C994973	Antiy-AVL	Trojan(Backdoor).MSIL.Bladabindi.as
Arcabit	Generic.MSIL.Bladabindi.9C994973	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.9C994973
BitDefenderTheta	Gen.NN.Zemslf.36276.bmW@a0BZiCp	Bkav Pro	W32.AIDetectNet.01

### E. Analisis

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 tentu 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.

Perbedaan Malware, Virus, dan Trojan, Berbagai jenis malware memiliki sifat dan karakteristik yang unik. Jenis-jenis malware antara lain sebagai berikut:

- Virus adalah jenis malware paling umum yang dapat mengeksekusi dirinya sendiri dan menyebar dengan menginfeksi program atau file lain.
- Worm dapat menggandakan diri tanpa program host dan biasanya menyebar tanpa interaksi apa pun dari pembuat malware.

- Trojan Horse dirancang untuk tampil sebagai program perangkat lunak yang sah untuk mendapatkan akses ke sistem. Setelah diaktifkan setelah penginstalan, Trojan dapat menjalankan fungsi jahatnya.
- Spyware mengumpulkan informasi dan data pada perangkat dan pengguna, serta mengamati aktivitas pengguna tanpa sepengetahuan mereka.
- Ransomware menginfeksi sistem pengguna dan mengenkripsi datanya. Penjahat dunia maya kemudian meminta pembayaran tebusan dari korban sebagai imbalan untuk mendekripsi data sistem.
- Rootkit memperoleh akses tingkat administrator ke sistem korban. Setelah terinstal, program memberikan akses root atau hak istimewa kepada pelaku ancaman ke sistem.
- Virus backdoor atau Trojan akses jarak jauh (RAT) secara diam-diam membuat pintu belakang ke dalam sistem komputer yang terinfeksi yang memungkinkan pelaku ancaman untuk mengaksesnya dari jarak jauh tanpa memberi tahu pengguna atau program keamanan sistem.
- Adware melacak browser pengguna dan riwayat unduhan dengan maksud untuk menampilkan iklan pop-up atau spanduk yang memikat pengguna untuk melakukan pembelian. Misalnya, pengiklan mungkin menggunakan cookie untuk melacak halaman web yang dikunjungi pengguna untuk menargetkan iklan dengan lebih baik.
- Keyloggers, juga disebut monitor sistem, melacak hampir semua yang dilakukan pengguna di komputer mereka. Ini

termasuk email, halaman web yang dibuka, program, dan penekanan tombol.

Lalu pada praktikum kali ini menggunakan metode OSINT untuk melakukan analisis malware. 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.

Beberapa teknik yang digunakan untuk mengumpulkan dan memproses Open Source Information

- 1) Pertama, strategi dan framework harus jelas untuk memperoleh dan menggunakan Open Source Intelligence. Tidak disarankan untuk menggunakan pendekatan OSINT dengan perspektif sendiri walaupun kita dapat menemukan sesuatu informasi yang menarik atau bermanfaat. Dengan banyaknya informasi yang tersedia melalui sumber terbuka hanya akan membuat kita kewalahan jika tidak menggunakan framework yang jelas. Sebagai gantinya, kita harus tau persis apa tujuan kita menggunakan OSINT, misalnya untuk mengidentifikasi atau memulihkan kelemahan pada jaringan kita, dan kemudian memfokuskan pencarian secara khusus untuk tujuan tersebut.
- 2) Kedua, kita harus mengidentifikasi perangkat atau tools dan teknik yang digunakan untuk mengumpulkan dan memproses

Open Source Information. Tanpa adanya perencanaan yang jelas, dan dengan jumlah informasi yang tersedia terlalu besar maka prosesnya menjadi tidak efektif.

Secara umum, pengumpulan Open Source Information terbagi dalam dua kategori yakni passive collection dan active collection.

- a) Passive Collection sering melibatkan penggunaan Threat Intelligence Platform untuk menggabungkan berbagai threat ke dalam suatu lokasi yang mudah diakses. Beberapa solusi Threat Intelligence lainnya yakni dengan menggunakan Artificial Intelligence, Machine Learning, Deep Learning, dan Natural Language Processing (NLP) yang memproses secara otomatis dalam memprioritaskan keputusan sesuai dengan kebutuhan dan tujuan dalam melakukan pengumpulan dan analisa informasi.

Terkadang dengan cara yang sama, beberapa komunitas “hacker” terkadang menggunakan botnet untuk mengumpulkan informasi berharga dengan penggunaan teknik traffic sniffing, keylogging.

- b) Active collection juga menggunakan berbagai macam teknik untuk mencari informasi spesifik. Untuk para Security Professional, jenis pekerjaan untuk mengumpulkan informasi biasanya dilakukan karena alasan : Alert yang dikumpulkan secara pasif telah ditandai sebagai sebuah yang berpotensi ancaman dan sebuah informasi yang diperlukan kemudian. Fokus dari pengumpulan intelligence sangat spesifik, seperti

percobaan-percobaan yang dilakukan oleh seorang penetration tester.

Pada praktikum yang dilakukan menggunakan software njRAT ini jika sudah terhubung dengan computer victim terdapat beberapa fungsi yang bisa dijalankan melalui host :

- 1) Manager, host bisa mengakses dan mengelola file dan folder pada victim.
- 2) Run File, akses shell jarak jauh pada victim, maka host bisa menjalankan perintah pada sistem tersebut.
- 3) Remote Desktop, host bisa mengendalikan sistem yang terinfeksi dari jarak jauh melalui remote desktop.
- 4) Remote Cam, host mendapat akses webcam dan mikrofon pada victim, sehingga memungkinkan penyerang untuk merekam video dan audio.
- 5) Keylogger, host bisa mendapatkan informasi sensitif seperti username dan password.
- 6) Get Password, host mendapat password tersimpan pada browser web dan klien email.

Setelah itu dilakukan scan malware pada web web mendapatkan hasil terbaik pada jotti 13/14 dan juga polyswarm 14/17 dengan selisih paling sedikit maka semakin sedikit hasil yang ada juga semakin akurat dan hasil terburuk VirSCAN dengan hasil 25/46 karena terlalu banyak selisihnya.

Jawab :

- 1) Port default yang digunakan oleh njRAT adalah = 5520
- 2) Apa alamat IP mesin tempat njRAT dihosting? = IPv4 Address

## **F. Kesimpulan**

Pada praktikum kali ini memiliki kesimpulan :

1. Malware adalah software yang dirancang khusus untuk bekerja secara tersembunyi dengan tujuan merusak perangkat dan mencuri data
2. OSINT adalah sebuah praktik mengumpulkan informasi dari sumber yang dipublikasikan atau tersedia untuk umum
3. Firewall sangat penting dalam mencegah adanya malware

## DAFTAR PUSTAKA

Malwarebytes. (2020). *What is malware? Definition and how to tell if you're infected*. Malwarebytes. <https://www.malwarebytes.com/malware>

Lutkevich, B. (n.d.). *What is malware? Definition from SearchSecurity*. SearchSecurity.

<https://www.techtarget.com/searchsecurity/definition/malware>

*Apa itu OSINT (Opent Source Intelligence) ? - CSIRT UMM*. (2022, June 11).

<https://csirt.umm.ac.id/2022/06/apa-itu-osint-opent-source-intelligence/#:~:text=OSINT%20umumnya%20merupakan%20metode%20pengumpulan>

Bule, G. (2020). *A Guide To Open Source Intelligence (OSINT)*. ITSEC.

<https://www.itsec.id/blog-post-osint-guide-part-1.html>

*Open-Source Intelligence (OSINT)*. (n.d.). Cyber. Retrieved March 6, 2023, from

<https://student-activity.binus.ac.id/csc/2022/04/open-source-intelligence-osint/>

*Apa Itu OSINT (Open Source Intelligence)? - Monitor Teknologi*. (2020,

November 23). [Www.monitorteknologi.com](http://www.monitorteknologi.com).

<https://www.monitorteknologi.com/apa-itu-osint/>