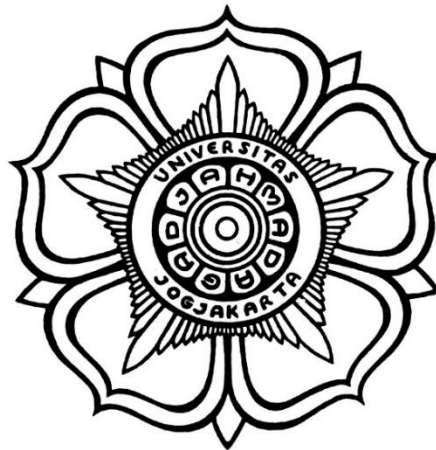


LAPORAN PRATIKUM
KEAMANAN INFORMASI 1
UNIT 4
PERTEMUAN 3



Disusun Oleh

Nama	:Riva Mahyuli
NIM	:21/478709/SV/19365
Kelas	:R1AA
Dosen	:Anni Karimatul Fauziyyah, S.Kom., M.Eng.

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNOLOGI DAN INFORMATIKA
UNIVERSITAS GADJAH MADA
2022/2023

UNIT 4

Analisis Anatomy Malware

A. Tujuan

- Meneliti dan menganalisis malware

B. 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.

C. Alat dan Bahan

- PC dengan akses internet

D. 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. Contoh jenis malware antara lain: Ransomware, Trojan, Hoax, Adware, Malware, PUP, Exploit, Exploit Kit dan Kerentanan. Cari malware dengan mengunjungi situs web berikut menggunakan istilah pencarian berikut:

- Dasbor Lanskap Ancaman Pusat Ancaman McAfee
- Pusat Ancaman Malwarebytes Labs (10 Malware Teratas)
- Securityweek.com > ancaman virus > virus-malware
- Technewsworld.com > keamanan > malware

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.

E. TUGAS/ LANGKAH PRATIKUM

1. Jenis-Jenis Malware :

Ransomware – Malware ini dirancang untuk menahan sistem komputer atau data di dalamnya hingga tebusan dibayar. Biasanya ransomware bekerja dengan mengenkripsi data di komputer dengan kunci yang tidak diketahui oleh pengguna. Beberapa versi lain ransomware dapat memanfaatkan kerentanan sistem tertentu untuk mengunci sistem. Ransomware tersebar melalui file yang diunduh atau beberapa kerentanan perangkat lunak.

Trojan horse - Trojan horse adalah malware yang menjalankan operasi berbahaya dengan menyamar sebagai operasi yang diinginkan. Kode berbahaya ini mengeksploitasi hak istimewa pengguna yang menjalankannya. Sering kali, Trojan horse ditemukan di file gambar, file audio, atau permainan. Trojan horse berbeda dari virus karena melekatkan diri ke file yang tidak dapat dijalankan.

Adware – Perangkat lunak didukung iklan yang dirancang untuk secara otomatis menampilkan iklan. Adware sering terinstal bersama beberapa versi perangkat lunak. Beberapa adware dirancang hanya untuk menampilkan iklan namun lazim juga ditemukan adware yang disertai spyware.

Malware adalah singkatan untuk Malicious Software (Perangkat Lunak Berbahaya). Malware adalah setiap kode komputer yang dapat digunakan untuk mencuri data, melewati kontrol akses, serta menimbulkan bahaya terhadap atau merusak sistem.

PUP adalah singkatan dari Potentially Unwanted Program, dalam artian adalah program yang terunduh meskipun tidak diinginkan oleh pengguna tersebut, contohnya seperti Adware ataupun Spyware. Biasanya PUP ini akan menumpang/disisipkan pada aplikasi/software gratis yang diinstal oleh pengguna, aplikasi/software ini biasa disebut Freeware. PUP dengan Malware adalah dua hal yang berbeda. Malware terinstall tanpa adanya permission oleh penggunanya sementara PUP menumpang/disisipkan ke program lain

Eksplit adalah sebuah kode yang menyerang keamanan komputer secara spesifik. Eksploit banyak digunakan untuk penentrasi baik secara legal ataupun ilegal untuk mencari celah pada komputer tujuan. Bisa juga dikatakan sebuah perangkat lunak yang menyerang celah keamanan yang spesifik namun tidak selalu bertujuan untuk meluncurkan aksi yang tidak diinginkan.

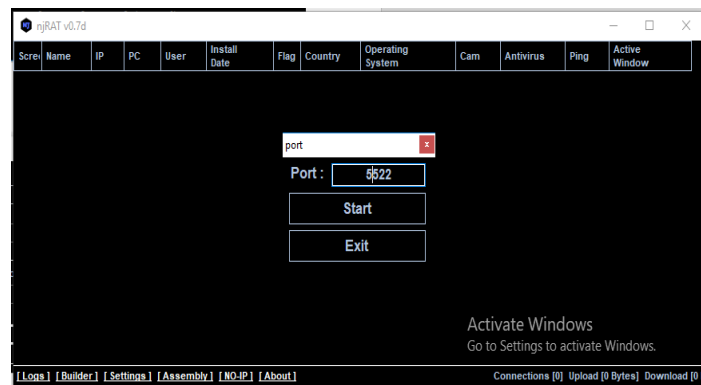
Exploit kits adalah sebuah alat yang mempermudah seseorang tanpa kemampuan dan pengalaman dalam penulisan software untuk membuat dan mengkostumisasi malware yang mana nantinya akan di distribusikan. *Exploit kits* biasanya juga disebut dengan *infection kit*, *crimeware kit*, *DIY attack kit* atau *malware toolkit*.

2. Develop Malware Trojan dengan Njrat

1. Download dan ekstrak aplikasi NJRAT kemudian run aplikasi NJRAT pada komputer host. <https://github.com/adarift/njRAT/releases/tag/v0.7D>

Name	Date modified	Type	Size
Icons	23/10/2020 14:49	File folder	
nj_users	28/02/2023 9:33	File folder	
Plugin	23/10/2020 14:49	File folder	
Stub	23/10/2020 14:49	File folder	
GeolIP.dat	23/10/2020 14:49	DAT File	1.137 KB
Lili	28/02/2023 9:20	Application	32 KB
NjRat 0.7D	23/10/2020 14:49	Application	8.745 KB
WinMM.Net.dll	23/10/2020 14:49	Application extens...	43 KB

2. Jalankan aplikasi Njrat yang telah didownload → Masukkan port yang ingin digunakan yaitu 5520 → start → Builder



3. Setelah itu cek IP address host, IP ini nantinya akan digunakan oleh NJRAT, dan pastikan juga komputer victim berada pada satu jaringan. Ethernet adapter ethernet → IPv4 Address

```
C:\Users\TAJ>ipconfig

Windows IP Configuration

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::d178:240c:fd9:1862%8
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet:

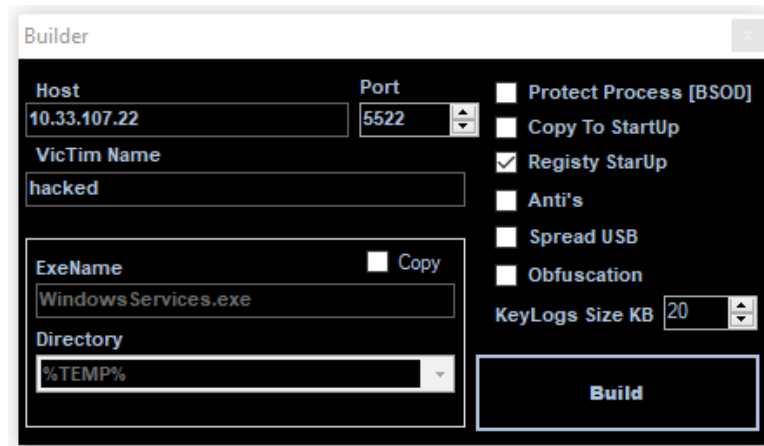
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::1cd7:1314:b1f:fb5%4
    IPv4 Address. . . . . : 10.33.107.22
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.33.107.254

Tunnel adapter Teredo Tunneling Pseudo-Interface:

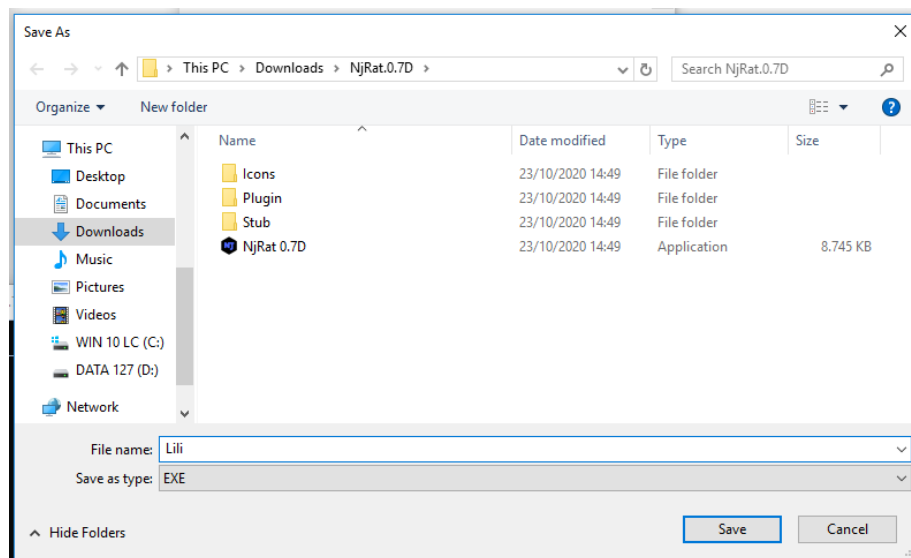
    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:0:2851:782c:2cf6:2793:f5de:94e9
    Link-local IPv6 Address . . . . . : fe80::2cf6:2793:f5de:94e9%13
    Default Gateway . . . . . : ::

C:\Users\TAJ>
```

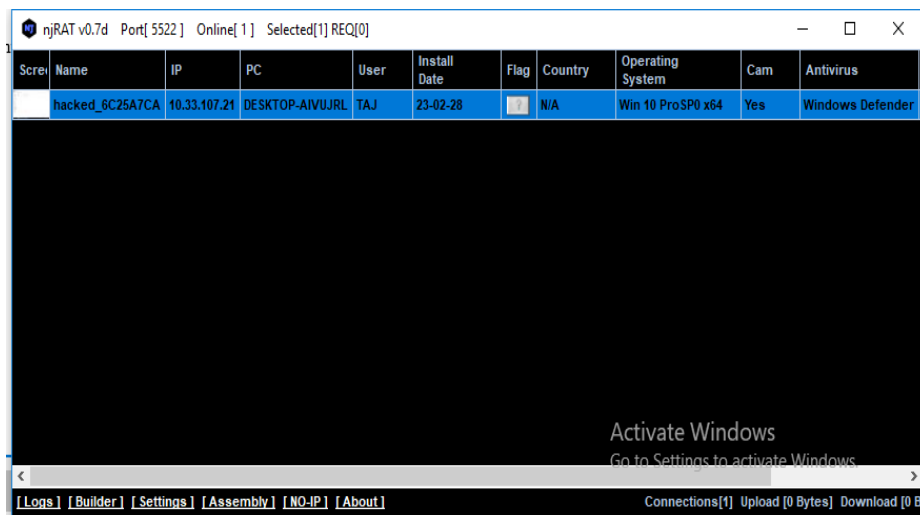
4. Buat aplikasi yang akan dipasang pada komputer victim. Masukkan IP Address host pada kolom host dan port yang sesuai dengan yang telah kita cek diawal agar dapat diakses oleh komputer nanti, kemudian klik tombol **Build**.



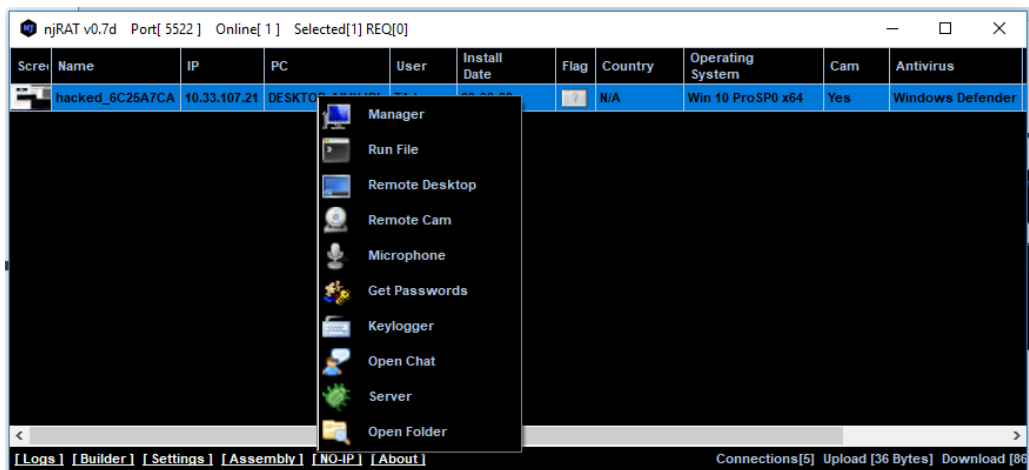
5. Simpan file, lalu kirimkan file ke target



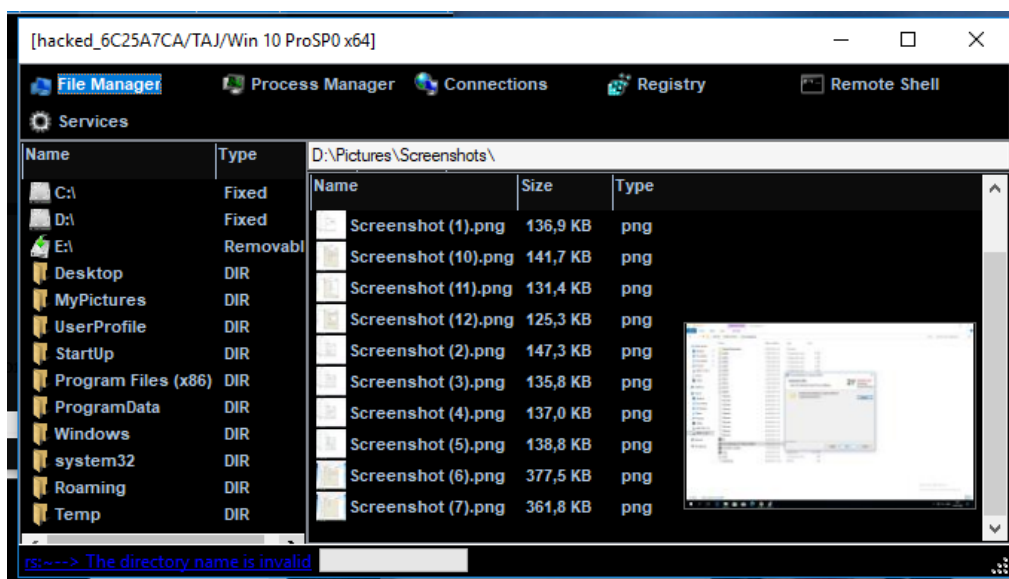
6. Setelah target menjalankan file yang telah kita buat, maka tampilan di PC kita akan menjadi seperti ini



7. Klik kanan untuk melihat menu, dibagian menu ini kita bisa melihat, meremote, mendengarkan, dan bahkan melihat seluruh file yang ada di PC korban tanpa diketahui



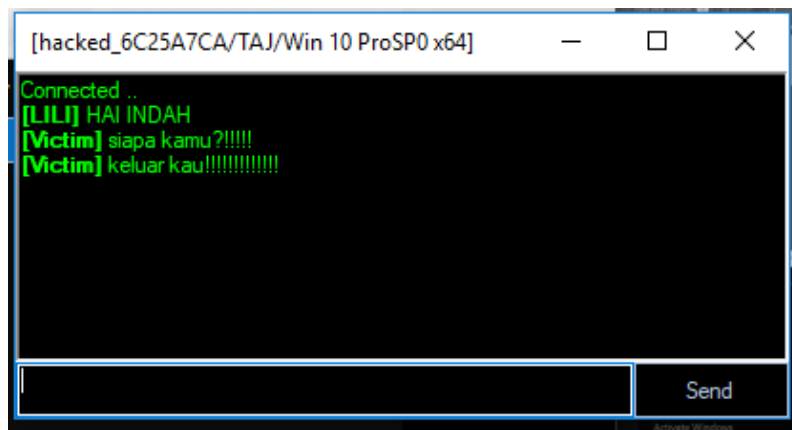
8. Manager untuk mengetahui semua folder yang terdapat di PC target



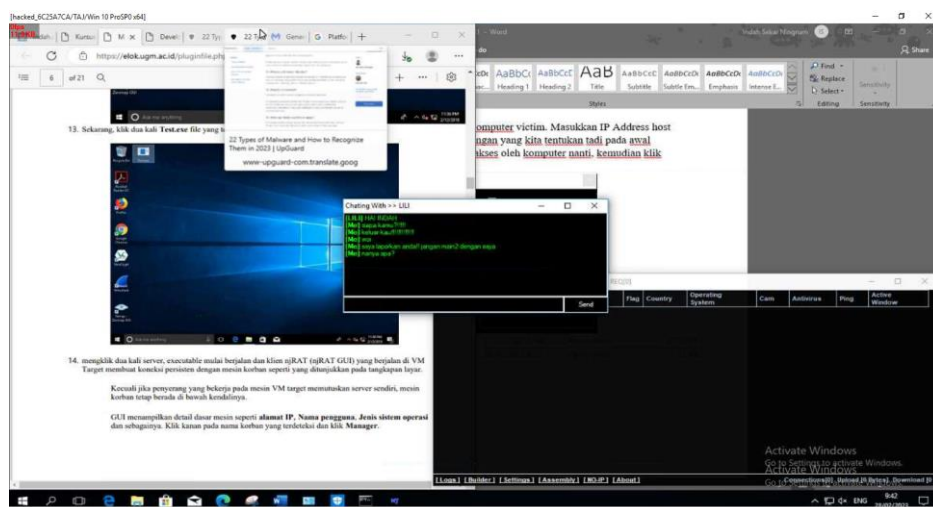
9. Remote cam untuk mengakses camera di pc target.









10. Open chat bisa digunakan pelaku untuk mechat korban yang langsung tertampil di PC korban.



11. Remote desktop untuk melihat desktop atau yang sedang dikerjakan target pada PCnya














12. Get password untuk melihat password yang telah digunakan pada PC tersebut







Pass				
UserName	Password	URL	App	User
 srilestari59		https://sso.ugm.ac.id/	FireFox	[hacked_6C25A7CA/TAJ/Win 10 ProSP0 x64]
 rahmawanto		https://sso.ugm.ac.id/	FireFox	[hacked_6C25A7CA/TAJ/Win 10 ProSP0 x64]
 indah.sekar0503		https://sso.ugm.ac.id/	FireFox	[hacked_6C25A7CA/TAJ/Win 10 ProSP0 x64]
 srilestari59		https://sso.ugm.ac.id/	FireFox	[hacked_6C25A7CA/TAJ/Win 10 ProSP0 x64]
 rahmawanto		https://sso.ugm.ac.id/	FireFox	[hacked_6C25A7CA/TAJ/Win 10 ProSP0 x64]
 indah.sekar0503		https://sso.ugm.ac.id/	FireFox	[hacked_6C25A7CA/TAJ/Win 10 ProSP0 x64]
Passwords(6)				

13. Kita juga bisa on/off PC target dari PC kita

njRAT v0.7d Port[5522] Online[1] Selected[1] REQ[0]

Screen	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam	Antivirus
	hacked_6C25A7CA	10.33.107.21	DESKTOP-AHGLUDU	TAJ	23.09.20		N/A	Win 10 ProSP0 x64	Yes	Windows Defender

 Manager
 Run File
 Remote Desktop
 Remote Cam
 Microphone
 Get Passwords
 Keylogger
 Open Chat
 Get Web
 Open Folder

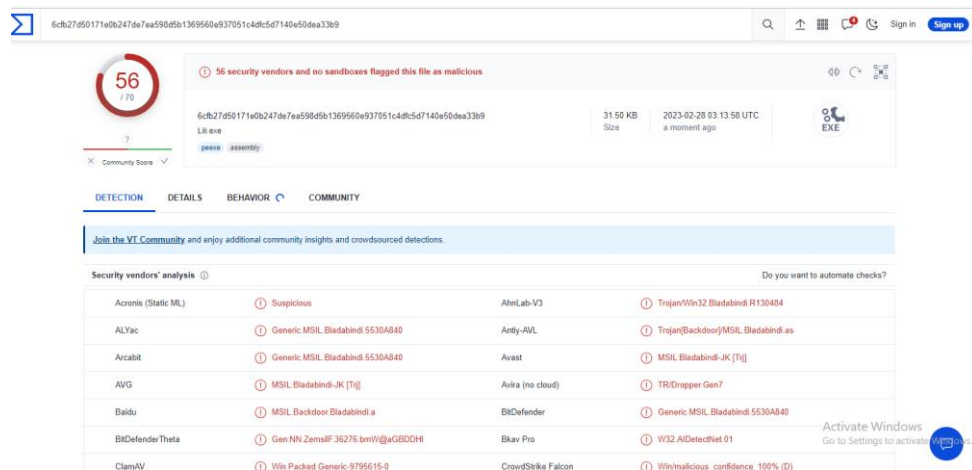
 Update
 Uninstall
 Restart
 Close
 Disconnect
 Rename

[Logs] [Builder] [Settings] [Assembly] [NO-IP] [About]

Connections[4] Upload [0 Bytes] Download [0 B]

3. Analisis Malware dengan Metode Osint

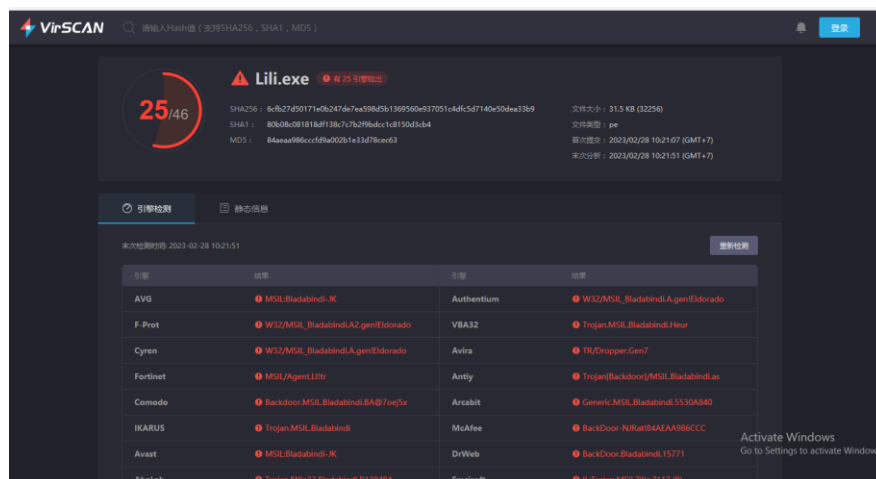
1. VIRUS TOTAL



The screenshot shows the VirusTotal web interface for a file named 'Lili.exe' (SHA256: 6cb27d50171e0b247de7ea596d5b1369560e937051c4dc5d7140e50dea33b9). The file is 31.50 KB and was uploaded on 2023-02-28 03:13:58 UTC. It has a score of 56/70. The 'DETECTION' tab is active, showing a table of security vendors' analysis. The table lists 16 vendors and their detection results for the file.

Security vendors' analysis	Do you want to automate checks?
Acronis (Static ML)	⚠ Suspicious
ALYac	⚠ Generic:MSIL_Bladabindi.5530A840
Arcabit	⚠ Generic:MSIL_Bladabindi.5530A840
AVG	⚠ MSIL_Bladabindi-JK [Trj]
Baidu	⚠ MSIL_Backdoor_Bladabindi.a
BitDefenderTheta	⚠ Gen:NN.Zemot.F.36276.bmW@uGBDDH
ClimAV	⚠ Win.Packed.Generic-9795615-0
AbnLab-V3	⚠ Trojan/Vin32_Bladabindi.R130484
Antiy-AVL	⚠ Trojan(Backdoor)MSIL_Bladabindi.as
Avast	⚠ MSIL_Bladabindi-JK [Trj]
Avira (no cloud)	⚠ TR/Dropper.Gen7
BitDefender	⚠ Generic:MSIL_Bladabindi.5530A840
BitDefender Pro	⚠ W32/AIDetectVet.01
CrowdStrike Falcon	⚠ Win.Malicious_confidence_100% (D)

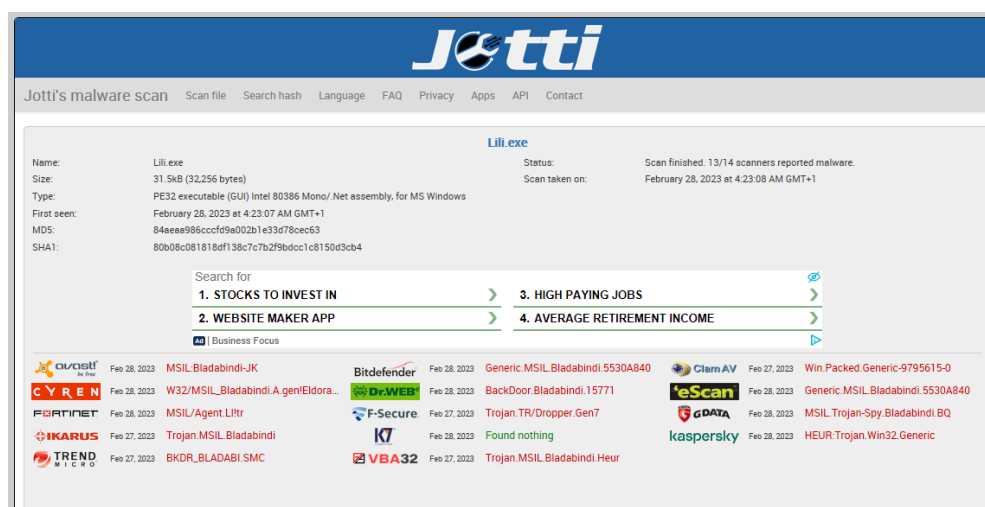
2. Virscan



The screenshot shows the VirSCAN web interface for a file named 'Lili.exe' (SHA256: 6cb27d50171e0b247de7ea596d5b1369560e937051c4dc5d7140e50dea33b9). The file is 31.5 KB (32256 bytes) and was uploaded on 2023-02-28 10:21:07 (GMT+7). It has a score of 25/46. The '引擎检测' (Engine Detection) tab is active, showing a table of engine detection results. The table lists 16 engines and their detection results for the file.

引擎	结果	引擎	结果
AVG	⚠ MSIL_Bladabindi-JK	Authentium	⚠ W32/MSIL_Bladabindi.A.gen/Eldorado
F-Prot	⚠ W32/MSIL_Bladabindi.A2.gen/Eldorado	VBA32	⚠ Trojan/MSIL_Bladabindi.Heur
Cyren	⚠ W32/MSIL_Bladabindi.A.gen/Eldorado	Avira	⚠ TR/Dropper.Gen7
Fortinet	⚠ MSIL/Agent.LITr	Antiy	⚠ Trojan(Backdoor)MSIL_Bladabindi.as
Comodo	⚠ Backdoor.MSIL_Bladabindi.BAB7095x	Arcabit	⚠ Generic:MSIL_Bladabindi.5530A840
IKARUS	⚠ Trojan.MSIL_Bladabindi	McAfee	⚠ BackDoor.NIRat.BA.AA.SB.CCC
Avast	⚠ MSIL_Bladabindi-JK	DrWeb	⚠ BackDoor.Bladabindi.15771

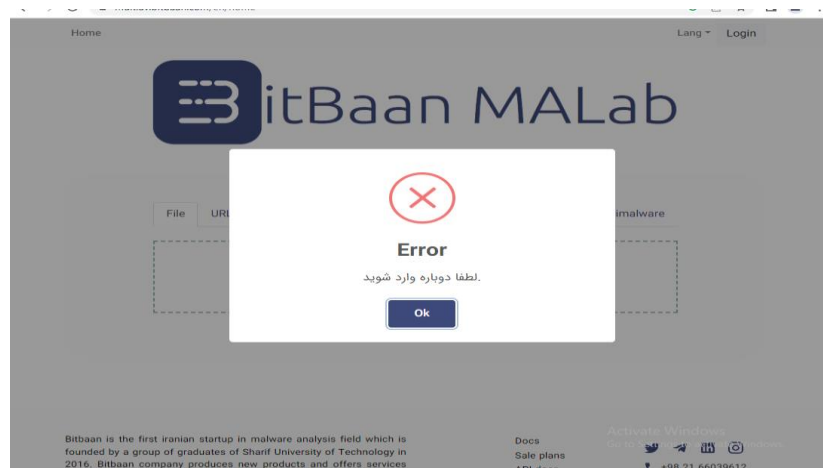
3. Jotti



The screenshot shows the Jotti's malware scan interface for a file named 'Lili.exe' (SHA256: 6cb27d50171e0b247de7ea596d5b1369560e937051c4dc5d7140e50dea33b9). The file is 31.5 KB (32256 bytes) and was uploaded on February 28, 2023 at 4:23:07 AM GMT+1. The scan finished on February 28, 2023 at 4:23:08 AM GMT+1. The scan results show 13/14 scanners reported malware. The results are displayed in a table with columns for the scanner name, the date, and the detection result.

Scanner	Date	Result
AVAST	Feb 28, 2023	MSIL:Bladabindi-JK
CYREN	Feb 28, 2023	W32/MSIL_Bladabindi.A.gen/Eldorado
FORTINET	Feb 28, 2023	MSIL/Agent.LITr
IKARUS	Feb 27, 2023	Trojan.MSIL_Bladabindi
TREND MICRO	Feb 27, 2023	BKDR_BLABABI_SMC
Bitdefender	Feb 28, 2023	Generic.MSIL_Bladabindi.5530A840
Dr.Web	Feb 28, 2023	BackDoor.Bladabindi.15771
F-Secure	Feb 27, 2023	Trojan.TR/Dropper.Gen7
K7	Feb 28, 2023	Found nothing
VBA32	Feb 27, 2023	Trojan.MSIL_Bladabindi.Heur
ClimAV	Feb 27, 2023	Win.Packed.Generic-9795615-0
eScan	Feb 28, 2023	Generic.MSIL_Bladabindi.5530A840
GDATA	Feb 28, 2023	MSIL.Trojan-Spy_Bladabindi.BQ
kaspersky	Feb 28, 2023	HEUR:Trojan.Win32.Generic

4. Bitbaan Malab



5. Poli swarm

