



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB	: KODE DAN AKTIVITAS MENCURIGAKAN
NAMA	: YEHEZKIEL STEPHANUS AUSTIN
NIM	: 215150207111053
TANGGAL	: 07/06/2023
ASISTEN	: JOSH ALEVSAN

Eksekusi Malware

1. Jalankan sistem operasi Linux (Desktop/Server) pada aplikasi Virtual Machine (VM),
2. Jalankan command berikut pada VM Terminal Anda:

```
sudo apt update && sudo apt install jd-gui # Debian  
paru -Sy --aur --noconfirm jd-gui-bin # ArchLinux
```

Note: jika tidak memiliki perintah `paru` didalam sistem, install menggunakan langkah berikut:

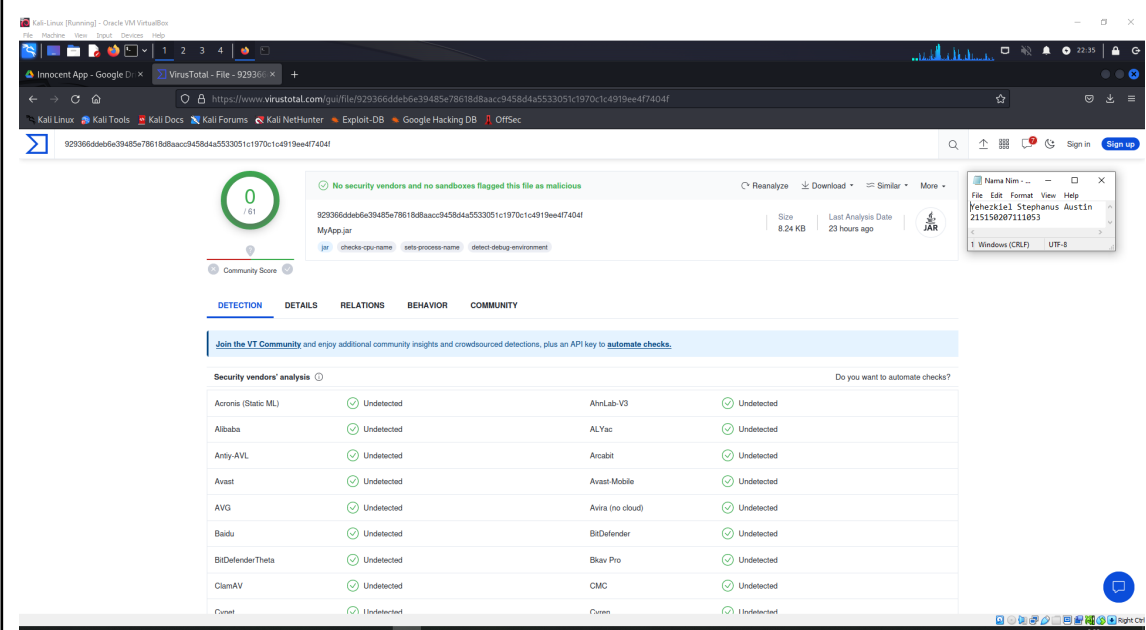
<https://github.com/Morganamilo/paru#installation>

3. Kemudian buatlah folder baru:

```
mkdir ~/victim_NIManda
```

4. Berikutnya, unduh file yang kita butuhkan, dan masukkan ke dalam folder yang telah kita buat sebelumnya, tautan *resource*, (**unduh file MyApp.jar**):
https://drive.google.com/drive/u/4/folders/1fcDWz_HVJpQvRnTWRGsDgF-egtlrOx4C

5. Masuk ke laman virustotal.com, kemudian upload file MyApp.jar ke dalam laman tersebut. **Jelaskan hasil yang diberikan dari virustotal tersebut.**



The screenshot shows the VirusTotal web interface for a file named 'MyApp.jar'. The file's SHA256 hash is 929366ddeb6a39485e78618b8aac94584a5533051c1970c1c4919ee47404f. The file size is 8.24 KB and it was analyzed 23 hours ago. A green circle with a '0' indicates that no security vendors or sandboxes have flagged the file as malicious. Below this, a table titled 'Security vendors' analysis' shows results from 19 vendors, all of whom have marked the file as 'Undetected'.

Vendor	Result
Acronis (Static ML)	Undetected
Alibaba	Undetected
Antiy-AVL	Undetected
Avast	Undetected
AVG	Undetected
Baidu	Undetected
BitDefender Theta	Undetected
ClamAV	Undetected
Cnnex	Undetected
AlmLab-V3	Undetected
ALYac	Undetected
Arcabit	Undetected
Avast-Mobile	Undetected
Avira (no cloud)	Undetected
BitDefender	Undetected
BitDefender Thida	Undetected
Bkav Pro	Undetected
CMC	Undetected
Cnnex	Undetected

Setelah MyFile.jar didownload dan dicek pada virustotal, dapat dilihat bahwa tidak terdapat virus pada file tersebut.

6. Kemudian, buka terminal anda dan masuk ke dalam path direktori tempat file MyApp.jar

```
cd ~/victim_NIManda
```

7. Tambahkan beberapa file (bebas) ke dalam folder tersebut.
8. Jalankan file MyApp.jar dengan perintah berikut:

```
java -jar MyApp.jar
```

Jelaskan apa yang terjadi pada file lainnya setelah program tersebut dijalankan.

```
(kali@Yehezkiel053)-[~/victim_215150207111053]
$ java -jar MyApp.jar
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Hello World!
```

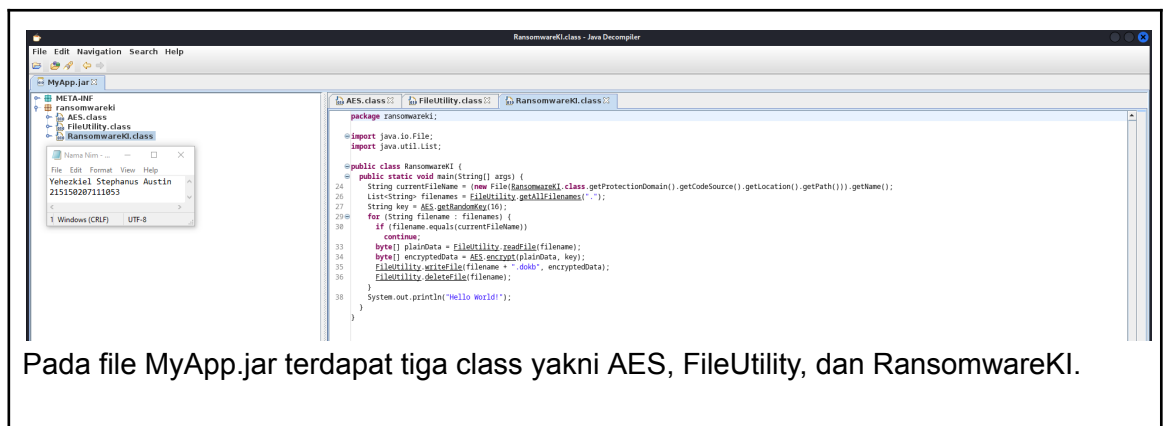
Setelah file MyApp.jar dijalankan, terlihat bahwa isi file tersebut adalah output Hello World!.

Analisa Malware

9. Berikutnya, kita jalankan decompiler tools yang telah kita install (jd-gui) melalui terminal dengan perintah:

```
jd-gui
```

10. Setelah jd-gui berhasil dijalankan masuk ke bagian file -> open file, kemudian pilih file MyApp.jar
11. Kemudian, kita lakukan analisa melalui jd-gui tersebut. File .class apa saja yang terdapat dalam file malware tersebut ?



12. Apa yang dilakukan FileUtility.class dalam file malware tersebut?

Kelas FileUtility digunakan untuk menyediakan beberapa utilitas untuk operasi berkas. Fungsi `readFile(String filename)` adalah fungsi untuk membaca isi dari suatu berkas dengan nama yang diberikan pada parameter. Lalu, fungsi `writeFile(String filename, byte[] data)` digunakan untuk menulis data ke dalam suatu berkas dengan nama yang diberikan pada parameter. Selanjutnya, fungsi `deleteFile(String filename)` adalah fungsi yang digunakan untuk menghapus suatu berkas dengan nama yang diberikan pada parameter. Dan terakhir terdapat fungsi `getAllFileNames(String directory)` yang digunakan untuk mendapatkan daftar semua nama berkas dalam suatu direktori yang diberikan.

13. Apa yang dilakukan AES.class dalam file malware tersebut, algoritma kriptografi apa saja yang digunakan dalam malware tersebut?

Kelas AES digunakan untuk melakukan enkripsi dan dekripsi dengan algoritma AES (Advanced Encryption Standard). Fungsi `setKey(String myKey)` adalah fungsi untuk mengatur kunci rahasia yang akan digunakan dalam enkripsi dan dekripsi. Lalu, fungsi `encrypt(byte[] plainData, String secret)` adalah fungsi untuk melakukan enkripsi data dengan menggunakan kunci rahasia yang telah ditentukan. Selanjutnya, terdapat fungsi `decrypt(byte[] encryptedData, String secret)` untuk melakukan dekripsi data yang telah dienkripsi sebelumnya. Dan terakhir terdapat fungsi `getRandomKey(int length)` untuk menghasilkan kunci rahasia acak dengan panjang yang ditentukan oleh parameternya.

14. Apa yang dilakukan RansomwareKl.class dalam file malware tersebut?

Kelas RansomwareKl adalah implementasi dari ransomware (jenis malware yang mengenkripsi berkas dan meminta tebusan). Fungsi `main(String[] args)` adalah fungsi untuk menjalankan proses enkripsi berkas.

Mitigasi dan Pemulihan dari Malware

15. Setelah kita melakukan analisa pada malware tersebut, kita dapat melakukan pemulihan kembali pada file kita yang terenkripsi.
16. **Unduh file 'Very Important Document.pdf.dokb'** dan masukkan ke dalam folder ~/victim_NIManda dari tautan Drive sebelumnya pada nomor 4.
17. Buatlah folder dengan nama 'result' di dalam folder ~/victim_NIManda.
18. Jalankan script code yang dapat membantu kita memulihkan salah satu file penting berjudul "Very Important Document.pdf.dokb" kembali menjadi file .pdf

script.py

```
from hashlib import sha1 # Import library kriptografi sha1
from Crypto.Cipher import AES # Import library kriptografi AES
import string # Bantuan lib string untuk import lowercase text

# Mengakses/membuka file yang terenkripsi
encryptedfile = open('Very Important Document.pdf.dokb', 'rb').read()

for i in string.ascii_lowercase:
    # Generate kunci dari tiap karakter a-z
    key = i * 16 # Pada tiap karakter akan digandakan sebanyak 16 misal 'aaaaaaaaaaaaaaaa'
    key = sha1(key.encode()).digest()[:16] # Mengambil 16 bytes pertama dari hasil SHA-1 digest bytes 0 sampai 15

    aes = AES.new(key, AES.MODE_ECB) # Membuat AES cipher dari key yang didapat dari SHA-1 digest sebelumnya
    menggunakan mode ECB
    result = aes.decrypt(encryptedfile) # Melakukan dekripsi file dengan algoritma kriptografi AES yang telah
    didefinisikan sebelumnya

# Pastikan terdapat direktori result
# Write file baru hasil proses dekripsi, seharusnya ada 26 file baru dan hanya ada 1 file yang dapat diakses.
open(f'result/Very Important Document_Char_{i}.pdf', 'wb').write(result)
```

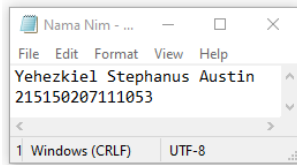
19. Jalankan kode yang telah anda buat, dan bukalah dokumen yang berhasil dipulihkan.

```
(kali@Yehezkiel053)-[~/victim_215150207111053]
$ python script.py
```

The key is: **97K9Bm8rkaVne5GNVJiO**

Once again, thank you for your prompt action and successful recovery of this document. Your outstanding efforts have made a meaningful difference. Oh, I almost forgot, here is the flag if you need it: **Flag{Cita-citaku_menj4di_5eor4ng_Malware_Analyst_p3nc4ri_cuan\$\$\$}**.

We are grateful for your assistance.



Sincerely,

Yesver

Dalam file tersebut, anda akan menemukan sebuah password juga. Password ini dapat kalian gunakan untuk menjalankan *decryptor* yang tersedia pada drive google yang ada pada nomor 4, apabila terjadi hal yang tidak diinginkan akibat malware tersebut.

9.5. EVALUASI

1. Malware jenis apa yang kita jalankan pada praktikum ini, dan jelaskan secara singkat bagaimana proses malware tersebut bekerja.

Ransomware adalah jenis malware yang dirancang untuk mengenkripsi file pada sistem komputer korban sehingga tidak dapat dibuka atau terbaca tanpa adanya kunci dekripsi yang tepat. Ransomware sering kali menggunakan algoritma enkripsi yang kuat, seperti AES, untuk mengubah struktur dan konten file menjadi bentuk yang tidak dapat dibaca atau diakses oleh pengguna.

2. Jelaskan bagaimana cara kerja kode script yang ada pada nomor 18, dalam men-dekripsi dan memulihkan file dari malware tersebut.

Kode script tersebut berfungsi untuk mendekripsi berkas yang dienkripsi oleh ransomware dengan menggunakan metode AES dalam mode ECB. Script tersebut mencoba semua kombinasi kunci rahasia yang mungkin berdasarkan karakter alfabet huruf kecil untuk mendekripsi berkas tersebut. Setelah berhasil mendekripsi, berkas hasil dekripsi disimpan dengan nama yang sesuai dengan karakter kunci rahasia yang digunakan.

3. Hal-hal apa saja yang kita perlu lakukan agar terhindar dari serangan malware

Disarankan untuk tidak mendownload file-file yang tidak jelas asal usulnya ataupun terlihat mencurigakan. Selain itu user juga harus berhati-hati dalam menjalankan sebuah file. User juga dapat menggunakan antivirus yang baik dan terpercaya untuk mencegah sebuah malware.