**Langkah Praktikum**

# Eksekusi Malware

1. Jalankan sistem operasi Linux (Desktop/Server) pada aplikasi Virtual Machine (VM)

|  |
| --- |
|  |

1. 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>

|  |
| --- |
| Penjelasan : Command diatas bertujuan memperbarui daftar paket dan menginstall JD-GUI (Decompiler Java).  sudo apt install jd-gui : untuk menginstall JD-GUI pada sistem |

1. Kemudian buatlah folder baru:

|  |
| --- |
| mkdir ~/victim\_NIManda |

|  |
| --- |
|  |

1. 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>

|  |
| --- |
| Penjelasan :  mv ~/Downloads/MyApp.jar ~/victim\_225150201111009/ : Command untuk memindahkan file dari downloads ke ~/victim\_225150201111009 |

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

|  |
| --- |
| Penjelasan :  Laporan VirusTotal untuk file "MyApp.jar" menunjukkan bahwa 2 dari 65 vendor keamanan menandai file ini sebagai mungkin berbahaya. Secara spesifik, Kaspersky dan ZoneAlarm oleh Check Point mengidentifikasi file tersebut dengan label HEUR:Trojan.Java.Alien.gen, menunjukkan deteksi heuristik dari kemungkinan trojan berbasis Java.  Analisis Vendor Keamanan:  **Ditandai**: Kaspersky dan ZoneAlarm oleh Check Point.  **Tidak Terdeteksi**: 63 vendor lainnya termasuk nama-nama terkenal seperti Avast, Acronis, Alibaba, ALYac, dan lainnya. |

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

|  |
| --- |
| cd ~/victim\_NIManda |

|  |
| --- |
|  |

1. Tambahkan beberapa file (bebas) ke dalam folder tersebut.

|  |
| --- |
|  |

1. Jalankan file MyApp.jar dengan perintah berikut:

|  |
| --- |
| java -jar MyApp.jar |

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

|  |
| --- |
| Penjelasan :  Program MyApp.jar hanya menampilkan pesan "Hello World!" tanpa melakukan tindakan mencurigakan terhadap file lain di dalam direktori victim\_225150201111009. Semua file tetap ada.  Namun ada penambahan ekstensi ".dokb" pada nama file Modul 9 - Kode dan Aktivitas Mencurigakan.pdf dan azusa.jpg. Ini adalah tanda adanya tindakan yang mencurigakan kedua telah dimodifikasi atau terenkripsi. |

# Analisa Malware

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

|  |
| --- |
| Jd-gui |

1. Setelah jd-gui berhasil dijalankan masuk ke bagian file -> open file, kemudian pilih file MyApp.jar
2. Setelah jd-gui berhasil dijalankan masuk ke bagian file -> open file, kemudian pilih file MyApp.jar

|  |
| --- |
| Penjelasan : : Program tersebut adalah kode ransomware yang menggunakan enkripsi AES untuk mengenkripsi file-file dalam sebuah direktori.  Saat program dijalankan, program akan mengenkripsi file-file dalam direktori tempat program dijalankan menggunakan kunci acak yang dihasilkan oleh AES.getRandomKey(16). Setelah mengenkripsi file, program akan mencetak "Hello World!" sebagai penanda bahwa proses enkripsi telah selesai. |

1. Kemudian, kita lakukan analisa melalui jd-gui tersebut.

File .class apa saja yang terdapat dalam file malware tersebut ?

|  |
| --- |
| * AES.class * FileUtility.class * RansomwareKI.class |

1. Apa yang dilakukan FIleUtility.class dalam file malware tersebut?

|  |
| --- |
| FileUtility.java: Kelas ini berisi utilitas untuk membaca, menulis, dan menghapus file. Metode readFile digunakan untuk membaca isi file ke dalam byte array, writeFile untuk menulis byte array ke dalam file, dan deleteFile untuk menghapus file. Metode getAllFilenames digunakan untuk mendapatkan semua nama file dalam sebuah direktori. |

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

|  |
| --- |
| AES.java: Kelas ini digunakan untuk mengenkripsi dan mendekripsi data menggunakan algoritma AES. Metode setKey digunakan untuk menginisialisasi kunci enkripsi. Metode encrypt digunakan untuk mengenkripsi data, sedangkan metode decrypt digunakan untuk mendekripsi data. |

1. Apa yang dilakukan RansomwareKI.class dalam file malware tersebut?

|  |
| --- |
| RansomwareKI.java: Kelas utama yang digunakan untuk menjalankan ransomware. Pada metode main, program akan mengenkripsi semua file dalam direktori kerja kecuali file ransomware itu sendiri. Setelah mengenkripsi, program akan menambahkan ekstensi ".dokb" pada nama file yang terenkripsi dan menghapus file aslinya. |

# Mitigasi dan Pemulihan dari Malware

1. Setelah kita melakukan analisa pada malware tersebut, kita dapat melakukan pemulihan kembali pada file kita yang terenkripsi.
2. **Unduh file ‘Very Important Document.pdf.dokb’** dan masukkan ke dalam folder ~/victim\_NIManda dari tautan Drive sebelumnya pada nomor 4.

|  |
| --- |
|  |

1. Buatlah folder dengan nama ‘result’ di dalam folder ~/victim\_NIManda.

|  |
| --- |
|  |

1. Jalankan script code yang dapat membantu kita memulihkan salah satu file penting berjudul “Very Important Document.pdf.dokb” kembali menjadi file .pdf

|  |
| --- |
| Penjelasan :  Program decrypt\_aes.py adalah skrip Python yang digunakan untuk mencoba mendekripsi file Very Important Document.pdf.dokb yang terenkripsi menggunakan algoritma AES dengan mode ECB. |

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

|  |
| --- |
| Screenshoot : |
| Flag : Flag{Cita-citaku\_menj4di\_5eor4ng\_Malware\_Analyst\_p3nc4ri\_cuan$$$} |

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 5, apabila terjadi hal yang tidak diinginkan akibat malware tersebut.

# Evaluasi

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

|  |
| --- |
| Malware yang dijalankan pada praktikum ini adalah Ransomware. Ransomware adalah jenis malware yang mengenkripsi file-file pada sistem korban, sehingga tidak dapat diakses oleh pengguna. Proses kerjanya adalah:   * Mengumpulkan semua nama file dalam direktori kerja kecuali file program itu sendiri. * Menghasilkan kunci acak untuk enkripsi. * Membaca setiap file, mengenkripsi kontennya menggunakan algoritma AES dengan kunci acak, dan menyimpan hasil enkripsi dalam file baru dengan ekstensi `.dokb`. * Menghapus file asli setelah konten terenkripsi disimpan. * Mencetak pesan "Hello World!" sebagai indikasi proses enkripsi selesai. |

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

|  |
| --- |
| Kode script pada nomor 18 menggunakan pendekatan brute force untuk mendekripsi file "Very Important Document.pdf.dokb" yang terenkripsi oleh ransomware. Script ini mencoba semua kemungkinan kunci enkripsi dengan panjang 16 karakter (hanya terdiri dari huruf kecil) secara berurutan. Untuk setiap kunci yang dicoba, script akan mencoba mendekripsi file menggunakan kunci tersebut dengan algoritma AES dalam mode ECB dan padding PKCS5. Jika hasil dekripsi valid (dalam hal ini, jika awalan file setelah didekripsi sesuai dengan header PDF), maka file hasil dekripsi akan disimpan dengan ekstensi `.pdf`. |

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

|  |
| --- |
| Beberapa hal yang dapat dilakukan untuk terhindar dari serangan malware:   * Menggunakan antivirus dan firewall yang selalu diperbarui. * Tidak membuka atau mengunduh file dari sumber yang tidak dipercaya. * Membuat cadangan data secara teratur. * Menggunakan email filtering untuk mencegah phishing. * Menjaga semua perangkat lunak selalu diperbarui dengan patch keamanan terbaru. * Menggunakan enkripsi untuk data penting. * Meningkatkan kesadaran keamanan dengan pelatihan bagi karyawan. * Menggunakan prinsip akses minimum yang diperlukan untuk mencegah penyebaran malware. |