# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang Masalah

Portable Document Format (disingkat PDF) adalah sebuah format berkas yang dibuat oleh Adobe Systems pada tahun 1993 untuk keperluan pertukaran dokumen digital. Format PDF digunakan untuk merepresentasikan dokumen dua dimensi yang meliputi teks, huruf, citra dan grafik vektor dua dimensi. Pada Acrobat 3-D, kemampuan PDF juga meliputi pembacaan dokumen tiga dimensi. PDF menjadi file yang sangat popular untuk digunakan, sehingga dengan banyaknya penggunaan file PDF muncul ancaman-ancaman yang dapat membahayakan pengguna khsusnya adalah pengguna komputer karena PDF merupakan file atau doktimen digital. Di mulai bulan September 2007, file PDF mulai dimanfaatkan oleh pembuat *malware* untuk menyertakan kode-kode tertentu dalam dokumen tersebut. Bentuk serangan tersebut berupa *trojan*. Seperti yang diberitakan Avira tanggal 6 Mei 2008, kelemahan *PDF* dimanfaatkan untuk menyisipkan kode malware, sehingga pada saat *PDF* dijalankan *malware* yang berupa *trojan* tersebut bisa melakukan instalasi dirinya ke komputer[28].

Serangan yang ditargetkan pada file PDF secara khusus menargetkan individu atau organisasi dan sering kali berisi beberapa elemen rekayasa sosial dalam upaya untuk membuatnya tampak seperti dari sumber yang sah, dan dengan demikian memikat pengguna yang ditargetkan untuk membuka dokumen PDF. Jenis serangan ini umumnya kurang signifikan jumlahnya dibandingkan dengan jenis serangan lain, dalam statistik hal ini disebabkan karena mereka hanya mempengaruhi satu atau sekelompok kecil orang. Dalam serangan yang ditargetkan agar dapat berhasil maka penyerang perlu melakukan penelitian dan perencanaan sebelumnya untuk mengumpulkan informasi individu atau organisasi tertentu dan, bergantung pada informasi yang dikumpulkan, konten manipulasi psikologis dipilih untuk digunakan dalam penyerangan[12].

Malware adalah software berbahaya yang tidak diinginkan, dan dirancang khusus untuk merugikan pengguna atau sistem target. Ini dapat mencakup jumlah jenis malware seperti *virus, trojan, backdoors, spyware, cryptolocker dan ransomware*. Pada saat ini malware telah mengalami perkembangan, malware bisa diklasifikasikan menurut fungsinya dan tujuan. Deteksi malware dapat dibagi menjadi empat kategori menurut jenis perilaku seperti penyebaran, infeksi, ketekunan, dan muatan. Perilaku kebanyakan merupakan salah satu serangan yang paling umum pada metode perangkat lunak berbahaya dan merujuk mekanisme untuk menyebarkan malware ketika ada komunikasi melalui internet atau ada hak akses didalamnya, ini juga merupakan perilaku tentang infeksi bagaimana malware menginfeksi sistem target[1]. Deteksi malware dapat dilakukan menggunakan platfom windows, deteksi perlu dilakukan karena menjadi bagaian terpenting untuk mencegah serangan malware. Untuk melakukan deteksi menggunakan windows, dibutuhkan software-software untuk menunjang proses deteksi. [6].

Oleh karena itu berdasarkan latar belakang di atas perlu diketahui bagaimana penyebaran malware dapat terjadi, maka dalam penelitian ini file yang berbentuk PDF akan dilakukan penyisipan baik dalam *proses infeksi* maupun *analisis*, serta teknik *infeksi malware* yang digunakan adalah *repackaging attack*. Teknik *repackaging attack*, yaitu metode yang digunakan dengan melakukan perubahan dan penyusupan pada file pdf, di dalam file pdf kemudian ditambahkan *payload* atau perintah berbahaya yang disusupkan dalam file. Hasil dari file yang *terinfeksi malware* dilakukan *analisis statis* untuk melihat apakah malware telah berhasil disisipkan dengan melakukan *uji deteksi* menggunakan *VirusTotal dan Any Run*. Maka dengan mengetahui *aktivitas malware* dapat memberikan manfaat bagi pengguna baik dalam menjaga file pdf dari *infeksi malware*, maupun menambah informasi tentang keamanan dari sebuah file.

### 1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, maka dapat dirumuskan permasalahan yang akan dibahas yaitu tentang, Bagaimana melakukan analisis

dan seteksi pada malware yang menginfeksi file pdf dengan menggunakan metode analisis static?.

## 1.3 Batasan Masalah

Adapun batasan masalah yang digunakan yaitu:

1. Penelitian ini hanya dilakukan untuk pengamatan terhadap *sampel malware* dan dampak serangannya, bukan untuk memperbaiki sistemnya.
2. Penelitian dilakukan *malware* yang menjangkit *file PDF*.
3. Tidak terpasang *anti-malware* pada platform *Windows Deffender*.
4. Proses eksekusi malware dijalankan pada platform Windows.
5. Analisis statis menggunakan *Tools VirusTotal* dan *App Any Run*.

## 1.4 Maksud dan Tujuan Penelitian

Adapun tujuan dari penelitian ini yaitu:

1. Mengetahui proses *analisis* pada *file PDF* yang terjangkit *malware* dengan menggunakan metode static analysis.
2. Melakukan deteksi dengan membandingkan *file PDF* yang terjangkit malware menggunakan tools *Virus Toltal* dan *App AnyRun*.
3. Memberikan informasi langkah pencegahan agar terhindar dari *infeksi malware* pada perangkat windows.

## 1.5 Metode Penelitian

Adapun metode penelitian yang digunakan adalah sebagai berikut :

1. Studi pustaka

   Teknik mengumpulkan data dan informasi dengan cara membaca serta mempelajari tentang analisis malware, *reverse engineering*, *penetration-testing* dan hal-hal yang berkaitan dengan proses infeksi dan deteksi *malware* untuk digunakan sebagai referensi dalam penelitian ini. Sumber studi pustaka dapat berupa, paper, buku, jurnal, atau makalah dan referensi lainnya.
2. Membangun *environment* dengan melakukan instalasi modul serta *library* yang akan dibutuhkan oleh tools agar dapat dijalankan untuk melakukan analisis sampel *file PDF* dalam penelitian ini.
3. Implementasi

Mengimplementasikan teknik *repackaging attack* untuk menyusupkan malware pada *File PDF* menggunakan *framework Metasploit*.

4. Analisis Data

   Kegiatan analisis dilakukan terhadap objek penelitian yaitu *File PDF* menggunakan *analisis statis*.

5. Penulisan laporan

   Pada tahap ini, semua temuan yang didapat selama proses *analisis statis* akan dimasukkan kedalam laporan akhir.

## 1.6 Sistematika Penulisan

Penulisan dalam laporan tugas akhir ini memakai sistematika pembahasan sebagai berikut:

BAB I PENDAHULUAN

Bab ini memuat latar belakang, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, metode penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisikan kajian dari penelitian terdahulu dan teori berupa pengertian dan definisi yang diambil dari kutipan jurnal, web, ataupun buku serta beberapa literature review yang berkaitan dengan penyusunan laporan tugas akhir ini.

BAB III METODOLOGI PENELITIAN

Bab ini mencakup metodologi penelitian yang memberikan gambaran dan alur dari penelitian yang dilakukan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan kebutuhan sistem dan hasil analisis malware sample dengan menggunakan metode static analysis.

BAB V KESIMPULAN DAN SARAN

Bab terakhir memuat kesimpulan dan saran keseluruhan dari bab sebelumnya sebagai hasil yang diperoleh yang diharapkan dapat bermanfaat dalam penelitian selanjutnya.