BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Serangan yang ditargetkan adalah PDF yang 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 kami karena sifatnya, mereka hanya mempengaruhi satu atau sangat sekelompok kecil orang. Agar serangan yang ditargetkan berhasil, penyerang melakukan penelitian dan perencanaan sebelumnya untuk mengumpulkan informasi tentang individu atau organisasi tertentu dan, bergantung pada informasi yang dikumpulkan, konten manipulasi psikologis dipilih untuk digunakan dalam penyerangan [28].

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. Namun, malware tidak terbatas pada ini, Malware bisa diklasifikasikan menurut fungsinya dan tujuan. Ini dapat dibagi menjadi empat kategori menurut jenis perilaku seperti penyebaran, infeksi, ketekunan, dan muatan. Perilaku kebanyakan adalah salah satu serangan yang paling umum metode perangkat lunak berbahaya dan merujuk mekanisme untuk menyebarkan malware ketika ada komunikasi melalui Internet atau ada hak akses didalamnya. Dan ini perilaku tentang infeksi bagaimana malware menginfeksi sistem target[1].

Deteksi malware pada platfom windows adalah prioritas terpenting dalam dunia ini untuk mencegah serangan malware. Dalam menggunakan windows, di butuhkan software-software untuk menunjang kegiatan pengguna dalam kegiatan sehari-hari. Namun seiring berjalannya waktu banyak software tentunya juga membuka celah keamanan baik melalui software itu sendiri maupun pengguna software itu tersebut[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 metode hybrid. Metode hybrid yang penulis terapkan pada penelitian ini yaitu teknik statis menggunakan virustotal dan teknik dinamis menggunakan platform 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.d

1.2 Rumusan Masalah

Merujuk uraian latar belakang diatas, maka dibuat rumusan permasalahan antara lain :

a. Bagaimana mekanisme analisa hybdrid untuk mengungkap file trojan yang sudah disusupkan pada file pdf?
b. Bagaimana hasil investigasi dari 2 metode analisa hybrid (static dan dinamic) dalam menganalisa file malware?

1.3 Batasan Masalah

Agar penelitian lebih terarah dan sesuai dengan rumusan masalah yang telah dipaparkan sebelumnya, maka peneliti membuat batasan masalah. Adapun batasan masalah yang ditetapkan adalah sebagai berikut :

a. Penelitian ini hanya dilakukan untuk pengamatan terhadap sampel malware dan dampak serangannya, bukan untuk memperbaiki sistemnya.
b. Penelitian dilakukan malware yang menjangkit file PDF.
c. Tidak terpasang anti-malware pada platform Windows Deffender.
d. Proses eksekusi malware dijalankan pada platform Windows.

e. Analisis statis menggunakan Tools VirusTotal dan Any Run.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah sebelumnya maka tujuan yang ingin dicapai dari penelitian adalah :

a. Mengetahui proses analisis malware dengan menggunakan metode Hybrid analisys.
b. Melihat perbandingan file PDF yang terjangkit malware menggunakan tools Virus Total dan Any Run.
c. Memberikan informasi langkah pencegahan agar terhindar dari infeksi malware pada perangkat windows.

1.5 Manfaat Penelitian

Metode penelitian dalam penulisan tugas akhir ini menggunakan metode static analysis yaitu penelitian yang dilakukan untuk mengetahui akibat yang ditimbulkan dari malware yang telah dieksekusi pada platform windows. Tahapan penelitian ini diantaranya :

a. Perumusan Masalah

   Tahapan ini memuat permasalahan yang menjadi landasan dilakukannya penelitian demi menjawab suatu masalah yang berkenaan dengan penelitian ini.

b. Pengumpulan Data

   Tahap ini merupakan proses pengumpulan data yang berkaitan dengan objek malware yang akan diteliti.

c. Studi Literatur

   Tahap ini merupakan proses mempelajari dan mengumpulkan data dari sumber yang relevan dan mendukung terhadap penelitian ini.

d. Observasi

   Tahap ini merupakan proses pengumpulan informasi dengan mengamati fenomena yang terjadi secara real di lapangan yang terkait dengan penelitian ini. Informasi yang didapat berupa statistik tingkat serangan malware yang terjadi dan sampel malware yang dijadikan objek penelitian.

e. Tahap Analisis

Tahap ini melakukan analisis malware dengan menganalisis Statis. Analisis malware ini dimulai dengan melihat kemungkinan adanya file yang diinfeksi malware pada objek yang diteliti, menjalankan objek malware yang diteliti guna melihat efek yang ditimbulkan oleh malware terhadap sistem file.

f. Dokumentasi

Tahap ini merupakan kumpulan data-data dan informasi hasil dari analisis yang dilakukan terhadap objek malware yang diteliti yang kemudian disusun kedalam laporan skripsi.

1.6 Sistematika Penulisan

Tujuan sistematika penulisan berisikan garis besar atau gambaran secara umum laporan penelitian ini sehingga mempermudah pemahaman alur isi. Adapun garis besar isi laporan skripsi sebagai berikut :

Bab I Pendahuluan, tahapan ini merupakan bab awal yang menjelaskan tentang latar belakang masalah penelitian, rumusan masalah, batasan masalah, tujuan penelitian, manfaat 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 berisikan gambaran umum tentang alur proses penelitian, prosedur dan mekanisme metode analisis yang diterapkan pada skenario kasus penelitian dan skenario kasus yang diterapkan pada penelitian.

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

Bab V Penutup, bab ini menjelaskan tahapan terakhir yang dilakukan peneliti dan memuat kesimpulan dari keseluruhan uraian dari bab-bab sebelumnya. Tahapan ini juga memaparkan kekurangan serta saran untuk pengembangan penelitian berikutnya.

Daftar Pustaka, berisi referensi terkait dengan penelitian ini, baik melalui ebook, publikasi jurnal, dan artikel situs yang dapat menunjang proses penelitian.