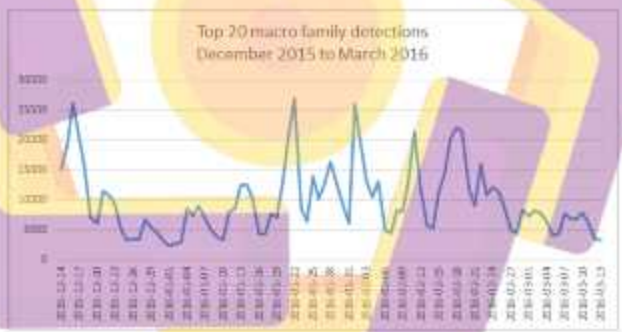
# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang Masalah

Microsoft Word merupakan perangkat lunak pengolah kata buatan Microsoft. Aplikasi ini memiliki beragam manfaat dan fungsi pada pekerjaan kantor, biasanya digunakan untuk membuat laporan, surat, dokumen, dan kebutuhan kantor lainnya. Salah satu contohnya adalah fungsi macro pada Word [1]. Walaupun memiliki fungsi beragam, sebagai user juga harus waspada dalam penggunaan aplikasi tersebut. Microsoft sendiri memberitahu bahwa ada celah yang dapat digunakan untuk menyisipkan virus kedalam suatu dokumen. Celah yang dapat dimanfaatkan adalah fungsi macro dari Word [2]. Terlihat data dari Microsoft pada Desember 2015 sampai Maret 2016, menunjukkan bahwa terdeteksi 20 malware macro teratas yang menginfeksi cukup banyak pengguna hanya dalam 3 bulan [3]. Seperti yang ditunjukkan pada **Gambar 1.1**.




**Gambar 1.1 Grafik Pendeteksian 20 Malware Macro** [3]

Menurut data dari Webroot pada Juni 2018, hampir 50% warga di Amerika tidak menggunakan antivirus. Hal ini pun dapat mempermudah lewatnya pengiriman file malware kepada korban [26]. User yang mematikan fitur ini biasanya tidak ingin kerepotan dikarenakan pertahanan yang terdapat dalam antivirus dan firewall terkadang menghambat berjalannya suatu aplikasi yang diinstal. Kerentanan dari pengaktifan macro ini dapat dimanfaatkan oleh

penyerang agar bisa mendapatkan akses ke komputer korban. Umumnya penyerang membuat suatu konten supaya menarik perhatian korban dan membuat kewaspadaan menurun. Setelah korban mengakses berkas yang berisi *malware* tersebut, penyerang mendapatkan kendali atas komputer target. Begitupun dalam penelitian ini, berkas malware macro terlihat seperti dokumen biasa. Pada saat berkas tersebut dibuka, akan muncul notifikasi pada word untuk mengaktifkan fungsi macro [4][5]. Setelah korban mengaktifkan fungsi tersebut, secara otomatis korban telah memberi alih kendali perangkat komputer yang dimilikinya kepada penyerang dari jarak dengan teknik *Remote Code Execution* [6]. Jika korban merasa telah terinfeksi malware, sebaiknya korban melakukan pendeteksian agar komputer yang dimiliki aman dari serangan.

Maka dari itu, diperlukan analisis terhadap malware agar mengetahui perilaku dan karakteristik. Hal ini dilakukan agar user mendapatkan data dari malware dan dapat menetukan langkah pencegahan terhadap malware tersebut.

Berdasarkan latar belakang masalah diatas, peneliti memuat sebuah topik penelitian dengan judul "Analisis dan Deteksi Malware Trojan pada Berkas Doc Menggunakan Metode Statis dan Dinamis". Penggunaan metode analisis statis bertujuan untuk meneliti source code malware tanpa menjalankan malware tersebut. Kemudian penggunaan metode analisis dinamis yang bertujuan untuk meneliti source code malware dengan menjalankan malware tersebut di lingkungan yang aman agar mengetahaui dampak langsung dari malware tersebut [7].

## 1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dibahas, maka dapat dirumuskan permasalahan yang akan dibahas yaitu:

1. Bagaimana cara menentukan antivirus yang baik untuk mengatasi malware trojan?
2. Bagaimana cara menemukan IP penyerang yang terhubung dengan korban?
3. Bagaimana cara melakukan pendeteksian bila terinfeksi malware trojan?

## 1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini yaitu:

1. Pengaksesan malware trojan diakses dengan Microsoft word 2013.
2. Pembuatan dan pengeksekusian malware menggunakan kali linux.
3. Proses exploit yang dilakukan dalam penelitian ini memakai sistem operasi Windows 7 pada VirtualBox.
4. Penelitian ini melakukan pengamatan dari serangan malware serta dampak yang diakibatkan.
5. Skenario serangan yang dibuat dalam penelitian ini mengasumsikan bahwa komputer target tidak terpasang antivirus dan firewall.
6. Proses analisis pada penelitian ini menggunakan tools Virustotal dan Anyrun.
7. Malware yang menjalankan exploit pada penelitian ini berupa payload dengan tipe reverse tcp.

## 1.4 Tujuan Penelitian

1. Menentukan antivirus yang dapat mengatasi malware trojan dengan melakukan analisis statis.
2. Mencari tahu IP penyerang yang terhubung pada korban dengan melakukan analisis dinamis.
3. Melakukan pengecekan jaringan yang terhubung di windows menggunakan command prompt dan mengeksekusi malware trojan menggunakan task manager.

## 1.5 Metode Penelitian

Adapun metode penelitian yang dipakai dalam penelitian ini menggunakan metode dynamic analysis. Berikut adalah tahapan penelitiannya:

1. **Studi Literatur**

   Studi literatur dilakukan dengan membaca dan mempelajari sejumlah referensi yang berkaitan dengan pembuatan serta pengeksekusian malware.

2. **Observasi**

Tahap ini adalah proses pengumpulan informasi, dilakukan dengan pengamatan kinerja malware yang terjadi secara real time.

3. **Analisa Data**

   Tahap ini adalah tahap dilakukannya analisis malware dengan menganalisis secara statis dan dinamis. Analisis malware dimulai dengan melihat kemungkinan suatu berkas telah terinfeksi malware pada objek yang diteliti, menjalankan objek malware yang diteliti agar dapat melihat dampak yang ditimbulkan malware terhadap sistem berkas

## 1.6 Sistematika Penulisan

Penulisan Tugas Akhir ini disusun dengan sistematika penulisan sebagai berikut:

**BAB I PENDAHULUAN**

Pendahuluan berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, metode penelitian, dan sistematika penulisan.

**BAB II LANDASAN TEORI**

Bab ini memuat hasil studi pustaka mengenai teori dan konsep. Penjelasan materi yang tersedia berhubungan erat dengan topik laporan Tugas Akhir. Tinjauan pustaka berisi beberapa referensi hasil penelitian yang berkaitan dengan topik tugas akhir, dan diperoleh dari berbagai sumber.

**BAB III METODOLOGI PENELITIAN**

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

**BAB IV PEMBAHASAN**

Bab ini berisi tentang implementasi malware, analisa malware, dan pendeteksian malware. Data hasil akhir pengujian dapat berupa gambar, table, grafik, log system, dan lain-lain, dengan pembahasan.

**BAB V PENUTUP**

Bab ini berisi kesimpulan dari penelitian yang dilakukan, dan saran.

**DAFTAR PUSTAKA**

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