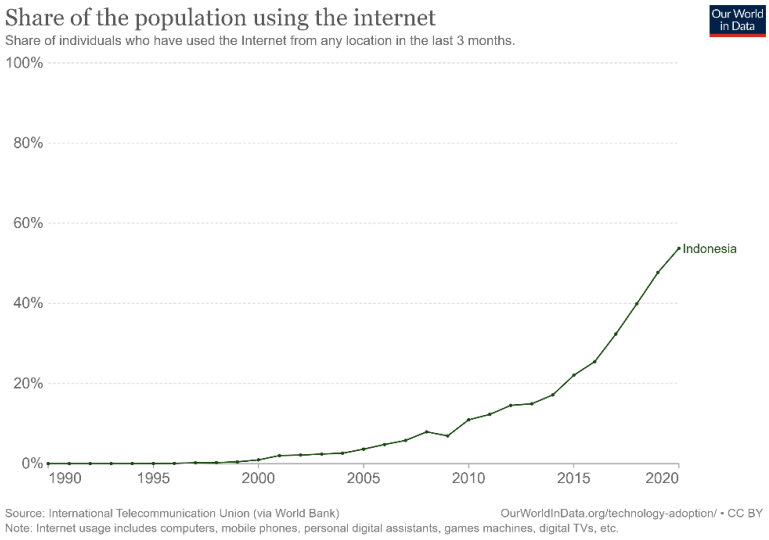
BAB 1 PENDAHULUAN

1.1 Latar Belakang Masalah

Pada masa ini, dunia teknologi pada sistem jaringan komputer merupakan bagian besar dari kehidupan dan tidak dapat dipisahkan dari dunia teknologi informasi, hal ini bisa kita lihat dari banyaknya pengguna jaringan komputer, internet. Pengguna internet di Indonesia meningkat setiap tahunnya seperti terlihat pada gambar data grafik dibawah (Gambar 1.1).



Gambar 1. 1 Data Grafik pertumbuhan populasi pengguna internet setiap tahun

Malware (*malicious software*) adalah perangkat lunak berbahaya yang dapat menyusup ke sistem operasi dan membuat sistem komputer berperilaku yang berbahaya seperti menggunakan sumber daya tanpa sepengetahuan pemilik perangkat, bahkan mengumpulkan informasi pribadi untuk dibagikan ke pihak ketiga tanpa persetujuan pengguna. *Malware-malware* dengan Teknik baru bermunculan seiring dengan perkembangan teknologi, ada banyak variasi *malware* yang dapat membahayakan pengguna seperti Trojan, virus, *adware*, *spyware*, *Ransomware* dan lainnya (Cahyanto et al., 2017). Pada penelitian ini peneliti akan melakukan analisis *malware* yang berjenis Trojan dan *spyware*. Dimana *malware* ini, bersifat menyamar dan

bersembunyi tanpa diketahui pengguna *computer* yang dapat membahayakan bocornya akun, *file* atau berkas yang bersifat penting.

Trojan dan *spyware* akan menginfeksi *computer* melalui banyak cara seperti email, menyamar seolah *software* yang baik, berupa link atau *file* lainnya. *Malware* ini dapat melihat data dan *file* penting bahkan aktivitas pada perangkat pengguna. Pada laporan BSSN mencatat peningkatan serangan oleh peretas. Hal ini sejalan dengan pengguna internet di masa pandemic Covid-19. BSSN melaporkan tercatat 88 juta serangan malware yang menyerang selama masa Januari – Agustus 2021 dan lebih banyak pada wujud malware, denial service ataupun kegiatan yang mengusik ketersediaan layanan sampai Trojan *activity* (CNN Indonesia/Dini Nur Asih, 2021). Trojan pernah menyerang Amazon pada tahun 2021 dan serangan jenis malware ini masih terus terjadi (Benefita, 2021).

Digital forensik adalah ilmu yang menerapkan identifikasi dalam kejahatan digital. Salah satu dalam mengidentifikasi tidak kejahatan tersebut yaitu mengumpulkan barang bukti berupa digital. Untuk menemukan jejak malware dibutuhkan analisis lebih spesifik dan mendetail sehingga dapat mendeteksi aktivitas malware. Analisis malware dapat dilakukan dengan tiga cara klasifikasi yaitu *static analysis*, *dynamic analysis dan hybrid analysis.*

Dalam penelitian ini, pertama peneliti akan membuat lingkungan yang aman seperti membuat *virtual machine* agar perangkat *computer* yang utama aman dari *malware*. Selanjutnya dilakukan analisis *malware* dengan metode *hybrid*, kombinasi metode statis dan dinamis. Dalam analisis statis dilakukan pengecekan pada *file* Trojan dan *spyware* tanpa menjalankan *malware* untuk melihat deskripsi dari *file malware* seperti *library* yang menggambarkan sifat kerja Trojan dan *spyware* saat dijalankan. Langkah selanjutnya adalah menganalisis dengan metode dinamis pada sampel *malware* dijalankan pada *virtual machine* yang terisolasi untuk melihat sifat dan perilaku *malware* yang dijalankan.

Trojan dan *spyware* akan di analisis menggunakan metode *hybrid analysis*, dengan metode ini dibutuhkan *tools* atau peralatan. yang diperlukan dalam penelitian analisis trojan dan *spyware* ini adalah PeStudio untuk analisis

statis dan SpyStudio untuk analisis dinamis. Pemilihan ini dikarenakan kemudahan dalam pengoperasiannya dalam menjalankan analisa.

Dari latar belakang penelitian ini penulis ingin melakukan analisis terhadap malware jenis Trojan dan *Spyware* dengan metode *hybrid analysis*, menggabungkan teknik analisis statis dan dinamis. Maka penulis memberi judul "Analisis Trojan dan *Spyware* Menggunakan Metode *Hybrid Analysis*".

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dipaparkan, maka rumusan masalah yang akan dibahas sebagai berikut:

1. Bagaimana perilaku Trojan dalam proses infeksi sistem komputer?
2. Bagaimana perilaku *Spyware* dalam proses infeksi sistem komputer?
3. Bagaimana proses analisis malware Trojan dan *Spyware* dengan menggunakan metode *hybrid analysis*?

1.3 Ruang Lingkup

Dalam penelitian ini, peneliti membatasi hanya membahas analisis yang dilakukan untuk pengamatan terhadap sampel *malware* jenis Trojan dan *Spyware* dan dampak serangannya terhadap sistem komputer melalui metode *hybrid analysis*.

1.4 Tujuan Penelitian

Adapun tujuan penelitian ini adalah untuk mengetahui dan mengimplementasikan proses analisis Trojan dan *Spyware* dengan menggunakan metode *hybrid analysis*, dengan menggunakan analisis gabungan analisis statis dan analisis dinamis.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat, baik secara praktis maupun teoritis.

1. Manfaat Praktis

1.1 Bagi Pembaca

Dapat menambah pengetahuan tentang proses penyerangan yang dilakukan Trojan dan *Spyware* terhadap sistem komputer agar berwaspada dan bisa mendeteksi virus tersebut lebih awal.

1.2 Bagi Peneliti

Memberikan penambahan wawasan dan pengetahuan tentang jenis-jenis *malware* terkhusus Trojan dan *spyware* dengan proses menyerangnya serta bagaimana cara mendeteksi *malware* pada perangkat lunak.

2. Manfaat Teoritis

Hasil penelitian ini diharapkan dapat memberikan informasi tentang proses analisis Trojan dan *spyware* dengan menggunakan metode *hybrid analysis*.

1.6 Luaran Yang Diharapkan

Berdasarkan latar belakang masalah yang telah penulis paparkan, maka luaran yang diharapkan adalah bagi pembaca agar dapat mengetahui bagaimana proses Trojan dan *spyware* menyerang dan menginfeksi perangkat atau sistem komputer dan jejak serangan tersebut dapat dijadikan bukti digital.

1.7 Sistematika Penulisan

Sistematika penulisan dari analisis Trojan dan *spyware* menggunakan metode hybrid analysis adalah:

BAB 1 PENDAHULUAN

Dalam bab ini yang berisi latar belakang masalah, rumusan masalah, ruang lingkup, tujuan dan manfaat penelitian, luaran yang diharapkan dan sistematika penulisan.

BAB 2 LANDASAN TEORI

Dalam bab landasan teori ini berisi uraian definisi dan teori-teori, metode, dan *tools* yang akan digunakan dalam penelitian.

BAB 3 METODOLOGI PENELITIAN

Dalam bab ini berisi tentang langkah-langkah yang nantinya digunakan untuk memecahkan permasalahan berdasarkan metode yang diusulkan dalam penelitian ini.

BAB 4 HASIL DAN PEMBAHASAN

Dalam bab ini berisi tentang pemrosesan dalam analisis atau pembahasan dan mengeluarkan hasil dari penelitian yang telah dilakukan dengan menerapkan metode yang telah diusulkan pada bab sebelumnya.

BAB 5 KESIMPULAN DAN SARAN

Dalam bab ini berisi tentang kesimpulan dari hasil proses analisis yang telah dilakukan dan saran untuk peneliti yang akan datang berdasarkan kekurangan dari apa yang telah dilakukan.

DAFTAR PUSTAKA

LAMPIRAN