BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi pada saat ini begitu pesat, semakin canggih teknologi maka semakin tinggi tingkat kejahatan di dunia maya maupun digital. Penyalahgunaan kecanggihan teknologi yang pesat salah satunya yaitu pengambilan data infomasi tanpa sepengetahuan pemiliknya. Saat sekarang salah satu ancaman yang sangat besar dan sangat merugikan bagi seseorang yaitu *malicious software* atau yang dikenal dengan sebutan *malware.*

Malicious software atau *malware* merupakan perangkat lunak yang secara eksplisit didesain untuk melakukan aktifitas berbahaya atau perusak lunak lainnya seperti Trojan, Virus, Spyware, dan Exploit[1]. *Malware* diciptakan dengan maksud tertentu yaitu melakukan aktifitas berbahaya yang berdampak sangat merugikan bagi para korbannya, antara lain seperti penyadapan serta pencurian informasi pribadi, hingga kasus perusakan sistem yang dilakukan oleh penyusup (*intruder*) terhadap perangkat korban dengan berbagai alasan. Salah satu media yang digunakan oleh *intruder* untuk mengendalikan komputer pengguna secara diam-diam dari jarak jauh adalah *malware* Poison Ivy, dikenal sebagai *trojan access remote* karena dapat memberikan kontrol penuh kepada *intruder* melalui pintu belakang (*backdoor*). Kemampuan *malware* Poison Ivy mengadopsi *software Remote Administration Tool* (RAT), yaitu kategori software yang baik (legal) yang dapat melakukan monitoring dan pengontrolan secara penuh. Contoh penggunaan software RAT ini biasa digunakan oleh seorang pimpinan perusahaan untuk mengontrol perangkat kerja (komputer) karyawannya melalui jaringan jarak jauh. Dengan fitur tersebut tidak jarang *malware* Poison Ivy dikatakan juga sebagai Software RAT yang illegal (RAT *malware*) dikarenakan tidak memberikan informasi berupa notifikasi saat proses remote terhubung (terhubung secara diam-diam), dengan *malware* sebagai medianya maka dalam hal ini merupakan sebuah bukti tindak kejahatan digital yang dilakukan oleh seorang *intruder*.

Pada penelitian sebelumnya yang dilakukan oleh Virgiawan A. Manoppo, Arie S. M Lumenta, dan Stanley D. S. Karouw (2020) telah dilakukan penelitian

analisis *malware* menggunakan analisis dinamis menggunakan Cuckoo Sandbox pada Jaringan Universitas Sam Ratulangi. Penelitian mereka melakukan simulasi perilaku dari program *malware* pada sebuah Jaringan di dalam Universitas dan dianalisa menggunakan Cuckoo Sandbox lalu bisa terlihat tingkat *malicious malware* berdasarkan hasil yang didapatkan dalam VirusTotal [2]. Kemudian penelitian berikutnya yang dilakukan oleh Triawan Adi Cahyanto, Victor Wahanggara, dan Darmawan Ramadana (2017) dilakukan penelitian analisis *malware* Poison Ivy menggunakan Regshot dan Cuckoo Sandbox didapatkan hasil bahwa Poison Ivy dapat dianalisis menggunakan metode analisis *malware* dinamis[3] .

Dengan adanya penelitian sebelumnya, pada tugas akhir ini dikembangkan penelitian dengan menambahkan 5 buah file *malware* baru untuk dianalisis selain Poison Ivy, yaitu : Trojan GenericKD 40427213, 32.Trojan.Raasmd.Auto, Dropped:Trojan.AgentWDCR.PZW, Gen:Variant.Strictor. 171520, dan Gen Variant Johnnie 97338. Metode yang akan digunakan adalah analisis *malware* dinamis dengan menggunakan Regshot dan Wireshark agar dapat diketahui bagaimana perilaku *malware* saat dijalankan.

Sistem Operasi Windows XP digunakan untuk penelitian ini karena beberapa pertimbangan. Pertama karena selama lebih dari 8 tahun semenjak diberhentikannya *support* untuk Windows XP, pengguna komputer di beberapa negara (seperti Armenia) masih menggunakan Windows XP. Dalam bulan desember 2022, penggunaan windows XP di negara seperti Armenia mencapai 63.94% diikuti dengan windows 10 dengan 22.79% [7]. Militer Amerika Serikat (US Army) hingga sekarang masih menggunakan Windows XP dan memutuskan untuk tidak meng-*upgrade* sistem operasi ini [6]. Windows XP masih digunakan oleh pengguna di seluruh dunia karena kemudahan penggunaan, performansi, dan stabilitas. Pertimbangan terakhir adalah karena Windows XP paling rentan diserang oleh malware [5].

Malware Trojan dan Gen digunakan dalam data statistik serangan *malware* bulan Juni-September 2022 yang dibuat oleh Securelist, *malware* yang paling banyak menginfeksi adalah Trojan dengan presentase 14.76%, dan diikuti dengan *malware* Gen yaitu dengan presentase 11.68%. [8].

1.2 Rumusan Masalah

Perumusan Masalah pada penelitian ini adalah

1. *Malware* manakah yang paling berbahaya diantara sample *malware* yang ada?
2. Bagaimana menganalisis *malware* menggunakan metode Analisis Dinamis?
3. Bagaimana cara menggunakan *Regshot* dan *Wireshark* untuk menganalisis *malware*?

1.3 Tujuan dan Manfaat

Tujuan dari Pembuatan Tugas Akhir ini adalah:

1. Dapat mengetahui *malware* mana yang paling berbahaya diantara sampel *malware* yang ada.
2. Dapat mengetahui cara kerja dan dampak yang ditimbulkan oleh *malware* menggunakan metode Analisis Dinamis.
3. Dapat mengetahui cara untuk menganalisis *malware* menggunakan Regshot dan Wireshark.

   Adapun manfaat dari penelitian Tugas Akhir ini adalah

   1. Memudahkan untuk pengguna komputer untuk memonitor dan menganalisa bagaimana cara kerja *malware* dan perilaku *malware*.
   2. Meningkatkan kesadaran para pengguna komputer akan bahayanya *malware*.
   3. Meningkatkan keamanan privasi pengguna komputer dalam penggunaan sehari hari.
   4. Memberikan rasa aman kepada pengguna komputer agar bisa mengidentifikasi *malware* pada sistem yang dipakai.

1.4 Batasan Masalah

Batasan masalah dari penelitian ini adalah:

1. Menggunakan metode Analisis Dinamis untuk menganalisa *malware*.
2. *Virtual Machine* yang digunakan untuk *environment malware sampling* adalah Oracle Virtual Box 6.1.32r149290.
3. Operating System yang digunakan adalah Windows XP Professional version 2002.

4. *Malware* yang dianalisa adalah sampel file *malware* Poison Ivy, Trojan GenericKD 40427213, 32.Trojan.Raasmd.Auto, Dropped:Trojan.Agent WDCR.PZW, Gen:Variant.Strictor.171520, dan Gen Variant Johnnie 97338, sampel-sampel ini dipilih karena termasuk *malware* yang umum dijumpai di jaringan komputer.
5. Aplikasi yang digunakan untuk menganalisa *malware* adalah Regshot 1.9.0 dan Wireshark 1.10.0.
6. Pengujian *registry check* oleh Regshot 1.9.0.
7. Pengujian *protocol* oleh Wireshark 1.10.0.

1.5 Metodologi Penelitian

Metode penelitian yang dilakukan dalam penelitian ini adalah sebagai berikut.

1. Studi Literatur

   Pada tahap ini, peneliti mencari dan mempelajari referensi-referensi yang berhubungan dengan perencaan dan penelitian yang akan dikerjakan dengan mengumpulkan penelitian-penelitian sebelumnya seperti buku, jurnal, internet dan referensi lain tentang *Virtual Machine, Malware, Malware Analysis*, Regshot, dan Wireshark.
2. Perancangan Sistem

   Pada Tahap ini Penulis merancang *sistem environment* yang akan digunakan untuk analisis *malware*, yaitu menggunakan *Virtual Machine Oracle Virtual* Box 6.1.32r149290 dan *Operating System* Windows XP Professional *version* 2002.
3. Pengujian Sistem

   Pada tahap ini penulis melakukan pengujian terhadap sampel file *malware*. Data yang digunakan adalah data sampel file Poison Ivy, Trojan GenericKD 40427213, 32.Trojan.Raasmd.Auto, Dropped:Trojan. AgentWDCR.PZW, Gen:Variant.Strictor.171520, dan Gen Variant Johnnie 97338. Aplikasi yang dipakai adalah Regshot dan Wireshark untuk proses analisis dinamis.

4. Analisis Sistem

   Pada tahap ini penulis melakukan analisis terhadap *malware* yang sudah dijalankan di dalam *virtual machine environment*.

5. Kesimpulan

   Pada tahap ini penulis mengevaluasi keseluruhan tahapan penelitian dan mendokumentasikan dalam bentuk laporan.

1.6 Sistematika Penulisan

Sistematika Penulisan Tugas Akhir ini adalah sebagai berikut:

- BAB I PENDAHULUAN

  Berisi latar belakang, tujuan penulisan, rumusan masalah, batasan masalah, metodologi penelitian, serta sistematika penelitian yang memuat susunan penulisan penelitian ini.

- BAB II TINJAUAN PUSTAKA

  Bab ini membahas landasan teori dan literatur yang digunakan dalam proses penelitian analisis dan deteksi *malware* menggunakan metode dinamis

- BAB III MODEL DAN PERANCANGAN SISTEM

  Bab ini berisi tahapan-tahapan yang dilakukan dalam proses penelitian berupa diagram alir penelitian, parameter yang menjadi referensi penelitian, dan desain rancangan setiap skenario.

- BAB IV ANALISIS SIMULASI SISTEM

  Bab ini berisi pembahasan hasil dari deteksi malware yang telah dilakukan. Pada bab ini juga berisi tentang analisi penulis.

- BAB V KESIMPULAN DAN SARAN

  Bab ini berisi kesimpulan dan saran Tugas Akhir untuk pengembangan selanjutnya