BAB I

PENDAHULUAN

1.1. Latar Belakang

Era serba digital saat ini, data menjadi sebuah aset yang sangat berharga. Berbagai macam teknik digunakan untuk mencuri data pribadi yang berpotensi disalahgunakan oleh pihak yang tidak bertanggung jawab. Salah satu contohnya yaitu maraknya penjualan data pribadi seseorang atau bahkan data milik instansi pemerintahan di forum *Darknet* yang dapat digunakan secara bebas bahkan secara cuma-cuma (Ciptohartono dan Dermawan, 2019). Hal ini disebabkan oleh kurangnya pemahaman dan kewaspadaan *user* terhadap keamanan data pribadi yang mereka miliki, sebagai contoh masih banyak *user* yang masih sembarangan mengunduh *software* yang tidak diketahui asalnya dan keamanannya.

Teknik yang dapat digunakan dalam penerapan tersebut menggunakan *malware* sebagai alat untuk mengambil data bahkan untuk sebuah sistem komputer melalui beberapa cara masuk seperti melalui lampiran pada *email*, *link* tautan, dan berbagai macam media digital lainnya (Septiani dkk, 2016). Teknik ini banyak sekali *user* yang telah menjadi korban pencurian data dengan menggunakan media *malware* ini yang memang sulit dikenali secara kasat mata oleh *user*, karena bentuk dari *malware* itu sangat beragam dan bisa berbentuk aplikasi yang sangat lazim digunakan oleh kebanyakan *user* seperti aplikasi berekstensi *.exe* yang penggunaannya banyak pada sistem operasi *Windows* 10 pada saat ini. Selain dapat mencuri data pribadi milik *user*, *malware* juga dapat mengganggu jalannya sebuah

sistem operasi dengan cara berjalan dilatar belakang sebuah sistem operasi yang tentu tidak dapat terlihat pada tampilan depan sistem operasi tapi dapat dirasakan dampaknya oleh *user* seperti menurunnya kinerja dari komputer *user*, terjadi malfungsi sistem operasi, hingga terkuncinya komputer sehingga tidak bisa digunakan oleh *user*.

Berdasarkan pada penelitian sebelumnya, *malware Hack.exe* menginfeksi suatu perangkat komputer dengan menempel pada suatu email yang ketika dibuka oleh pengguna *malware* tersebut akan menginfeksi dan berjalan dilatar belakang sistem tanpa diketahui oleh pengguna (Triantoro dkk, 2021). Penerapan *malware Njrat* bersifat sangat berbahaya yang dapat melakukan hak akses terhadap perangkat komputer korban termasuk membobol *web* dan kata sandi dengan cara serangan *malware* yang dilakukan oleh *attacker*. Perubahan terjadi pada *performance traffic* komputer yang terinfeksi *malware* menjadi semakin cepat, namun pada *network performance* akan semakin melemah saat sedang digunakan (Septiani dkk, 2016). Berdasarkan referensi yang sudah dituliskan diatas dapat diambil kesamaan yaitu dalam jenis *malware* yang sama yaitu *RAT* (*Remote Acces Trojan*), yang menjadi perbedaan dalam penelitian yang diambil saat ini adalah media inang atau *carier malware* tersebut dalam menginfeksi sebuah sistem yang dimana media yang infeksi *malware* pada penelitian ini melalui file dengan ekstensi (*.exe*) yang diunduh lalu dijalankan oleh pengguna PC.

Berdasarkan studi kasus yang telah dijelaskan, maka perlu adanya penelitian yang bertujuan untuk mengedukasi tentang bagaimana cara *malware* bekerja. Teknik pada penelitian ini adalah *Malware Analysis* menggunakan *Memory*

Forensics (Triantoro dkk, 2021) untuk mengetahui cara kerja *malware* yang menginfeksi penggunanya melalui file yang disisipkan pada sebuah surat elektronik (*e-mail*). Hasil kajian yang didapat bahwa banyak sekali *malware* yang menginfeksi penggunanya melalui file yang disisipkan pada file yang terlihat tidak mencurigakan, sedangkan pada penelitian ini *malware* yang diteliti menempel pada sebuah file yang berekstensi (.*exe*).

Era serba *online* banyak sekali menggunakan internet dan mengunduh berbagai macam aplikasi yang hal ini dapat digunakan oleh orang yang tak bertanggung jawab dalam menyisipkan *malware* terhadap sebuah file yang diunduh oleh pengguna *PC*. Objek yang digunakan pada penelitian ini adalah *AQUVAPRN.exe* yang memiliki jenis *malware RAT* (*Remote Access Trojan*) yang saat *malware* ini berjalan pembuat *malware* tersebut dapat mengambil data pribadi pengguna yang sistem operasinya terinfeksi (Cahyanto dkk, 2017).

Penerapan teknik ini bertujuan untuk mengetahui bagaimana cara kerja dari *malware AQUVAPRN.exe* dalam menginfeksi sebuah sistem operasi yang tidak terlihat hanya dengan kasat mata. Selain untuk melihat cara kerja *malware* tersebut, penelitian ini dapat menjadi acuan dalam mengetahui celah yang digunakan *malware* tersebut dalam menginfeksi sebuah sistem operasi yang digunakan oleh *user*. Harapan dari penelitian ini adalah mengetahui dokumentasi dari objek *malware* yang diuji yaitu *AQUVAPRN.exe*.

1.2. Rumusan Masalah

Berdasarkan latar belakang sebelumnya, maka rumusan masalah dari penelitian ini adalah:

1. Bagaimana cara kerja *malware AQUVAPRN.exe* bekerja pada suatu sistem operasi?
2. Seberapa banyak informasi seperti *file registry, create file, dan open file* yang dapat diketahui dengan menggunakan teknik *Memory Forensics* dari *malware AQUVAPRN.exe* ?

1.3. Tujuan Penelitian

Berdasarkan latar belakang dan rumusan masalah, maka tujuan penelitian ini adalah:

1. Mengetahui cara kerja *malware AQUVAPRN.exe* bekerja pada suatu sistem operasi,
2. Mengetahui banyaknya informasi seperti *file registry, create file, dan open file* yang terpengaruh dengan menggunakan metode *Memory Forensics* dari *malware AQUVAPRN.exe.*

1.4. Batasan Masalah

Batasan-batasan masalah yang ditentukan sebagai indikator untuk pencapaian target penelitian. Batasan masalah pada penelitian ini adalah:

1. Penelitian ini menerapkan metode *Memory Forensics* dalam investigasinya,

2. *Malware* yang digunakan pada penelitian berjenis *Remote Access Trojan* (RAT) dengan nama *AQUVAPRN.exe*,
3. Sistem operasi yang digunakan pada penelitian ini menggunakan *Windows* 10, dan
4. *Tools* yang digunakan pada penelitian ini adalah *IDA Pro*, *Virustotal*, dan *Any.run*.

1.5. Manfaat Penelitian

Manfaat yang diperoleh dari penelitian ini adalah:

1. Mengimplementasikan hasil studi kasus tentang sebuah *malware* pada sebuah sistem operasi,
2. Mengedukasi *user* dalam memahami cara kerja sebuah *malware* yang akan diinvestigasi, dan
3. Mengimplementasikan ilmu yang telah didapatkan selama perkuliahan *Malware Analysis* dan Keamanan Informasi.

1.6. Metodologi Penelitian

Metodologi penelitian yang dilakukan dengan menggunakan metode kualitatif berdasarkan riset penelitian terkait yang digunakan sebagai referensi. Adapun metode penelitian yang digunakan yaitu *Memory Forensics*.

1. Tahap Awal Penelitian

   Tahap awal penelitian merupakan tahap pertama saat melaksanakan sebuah penelitian. Tujuan dari tahapan tersebut untuk mencari penelitian dengan mempelajari literatur penelitian hingga melihat permasalahan yang terjadi

pada penelitian. Ada 2 (dua) cara dalam melakukan tahap awal dalam sebuah penelitian, yaitu:

a. Identifikasi Masalah

   Cara pertama pada awal penelitian, yaitu melakukan identifikasi masalah yang terjadi pada studi kasus penelitian terkait. Pemecahan masalah berupa ide dan solusi yang terjadi untuk mengatasi sebuah permasalahaan yang dapat diatasi.

b. Studi Literatur

   Cara kedua pada awal penelitian, yaitu mencari referensi teori yang berhubungan dengan studi kasus penelitian terkait. Studi literatur dapat dijalankan dengan teknis wawasan yang luas tentang objek yang akan diteliti.

2. Tahap Implementasi

   Tahap kedua merupakan proses penelitian yang mencakup dari berbagai aspek penelitain *malware* yang telah ditentukan sebelumnya. Metode tersebut digunakan saat penelitian *malware* menggunakan metode *Memory Forensics* memiliki tahapan sebagai berikut:

   a. *Static Analysis*,
   b. *Dynamic Analysis*,
   c. *Memory Forensics*, dan
   d. *Reverse Engineering*

3. Tahap Kesimpulan dan Evaluasi

Tahap terakhir merupakan tahapan paling akhir dalam hasil penelitian. Pada bagian tersebut akan mendapatkan inti dari pembahasan yang telah dipaparkan sebelumnya. Suatu upaya ketika penelitian tersebut telah mencapai tahap akhir akan diukur antara hasil atau dampak dari penelitian dengan tujuan yang telah tercapai.

1.7. Sistematika Penulisan

Sistematika penulisan yang digunakan dalam usulan penelitian adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini menjelaskan tentang garis besar penelitian terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini memuat tentang teori dasar yang digunakan dalam penelitian, perancangan, dan relevansi penelitian.

BAB III METODELOGI PENELITIAN

Bab ini berisi tentang metodelogi yang digunakan dalam pembahasan serta langkah langkah penyelesaian masalah dengan menggunakan metode yang digunakan dalam penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini akan membahas mengenai analisa yang dilakukan terhadap hasil pengumpulan, pengolahan dan analisa data yang diperoleh dari hasil penelitian.

BAB V KESIMPULAN DAN SARAN

Bab ini akan membahas mengenai kesimpulan yang diperoleh dari hasil penelitian dan analisa data yang telah dilakukan serta saran-saran yang dapat diterapkan dari hasil pengolahan data yang dapat menjadi masukan penelitian yang akan datang.