BAB I

PENDAHULUAN

1.1 Latar Belakang

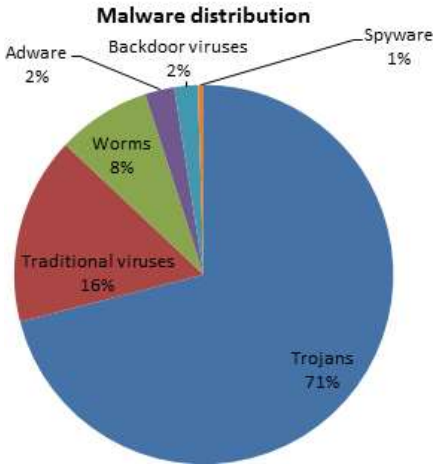
Modus kejahatan di dunia *cyber* saat ini sangat beragam. Teknik yang digunakan oleh penyerang semakin beragam dan kompleks. Berbagai serangan tersebut melibatkan *malicious software* atau yang biasa disebut *malware* yang merupakan suatu program jahat. Ancaman *malware* dan penyebarannya bisa melalui berbagai cara. Salah satu cara yang sering dilakukan untuk menyebarkan *malware* dengan cara menyisipkannya di sebuah aplikasi ataupun *file* tertentu. (Adenansi & Novarina, 2017).

Sebuah *malware* diciptakan untuk merusak atau membobol suatu *software* atau sistem operasi melalui *script* yang dirahasiakan, dalam arti lain disisipkan secara tersembunyi oleh penyerang. Perkembangan *malware* yang semakin pesat mengharuskan pengguna komputer semakin waspada agar informasi pribadi ataupun *file* yang penting tidak diambil oleh orang yang tidak berhak, demikian juga bagi para pelaku bisnis baik perusahaan maupun perorangan yang bergantung dengan sistem komputer untuk pekerjaannya agar lebih (Adenansi & Novarina, 2017).

Kemampuan untuk melakukan analisa *malware* bagi *investigator* menjadi tuntutan dalam setiap melakukan investigasi, hal ini dikarenakan meningkatnya jumlah *malware* serta evolusi dan mampu beradaptasinya terhadap perangkat analisis yang selama ini digunakan. Analisis *malware* membutuhkan keterampilan khusus untuk melakukan pendeteksian dan memahami cara kerja dari *malware* tersebut,

secara garis besar *malware* dibagi atas beberapa kategori yaitu, *worm, virus, trojan horse, adware,* dan *exploit*. Lima jenis *malware* tersebut merupakan jenis *malware* yang paling sering ditemukan pada analisis *malware* pada umumnya, yang dimana setiap kategori ini mempunyai spesifikasi atau cara kerja yang berbeda. (Muhammad, Sugiantoro, & Luthfi, 2017)

Laporan kuartalan menegaskan tingginya jumlah infeksi yang menyebar di seluruh mesin di seluruh dunia. Fakta bahwa jumlah ancaman baru meningkat secara signifikan dan pengajuannya meningkat 15% dibandingkan kuartal terakhir tahun 2010. Trojans dikenal sebagai jenis infeksi yang paling banyak menyebar di seluruh sistem komputer yang mencakup sekitar 70% dari semua *malware* yang terdeteksi, diikuti oleh *Virus* dan worm tradisional. (BullGuard, 2018)



Gambar 1.1 distribusi berbagai *malware*

Sumber: (BullGuard, 2018)

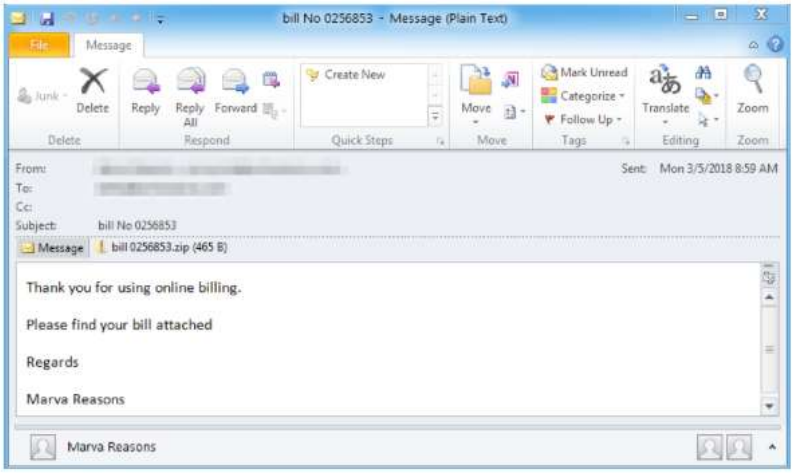
Sebuah *Trojan* melakukan akses jarak jauh yang sebelumnya tidak terdokumentasi telah terdeteksi di kedua serangan *email* yang ditargetkan secara

sempit dan kampanye besar-besaran. *Malware* yang terbaru menempatkan spin baru pada metode cybercrime lama sebagai pelaku ancaman mengeksplorasi cara-cara baru untuk menghasilkan uang tanpa menggunakan ransomware. (Sheridan, 2018)

Para analis Proofpoint telah menemukan *Trojan* akses jarak jauh yang sebelumnya tidak terdokumentasi yang disebut *Flawed ammyy* (Proofpoint Staff, 2018). *Malware Flawed ammyy* dibangun diatas kode Ammyy Adminversi versi 3 yang disalah gunakan. Ammyy Admin merupakan perangkat lunak desktop jarak jauh yang digunakan diantara jutaan konsumen dan bisnis untuk menangani *remote control* dan *diagnosis* pada platfom *Windows*, ini bukan pertama kalinya Ammyy Admin disalahgunakan, serangan Juli 2016 juga menggunakannya untuk menyembunyikan *malware* (Sheridan, 2018).

Penyerang yang mendistribusikan *Flawed ammyy* remote control trojan melalui kelompok peretas “TA505” yang terkenal karena mendistribusikan kampanye spam besar seperti Trojan Dridex perbankan, Locky ransomware, dan Jaff ransomware. (Saraswat, 2018).

FlawedAmmyy pada tanggal 5 Maret, pesan dikirim dari alamat spoofing domain penerima sendiri dengan subjek seperti "Tanda Terima No 1234567" (digit acak, dan kata pertama juga bisa "Bill" atau "Faktur") dan lampiran yang sesuai "Tanda Terima 1234567.zip ". Lampiran adalah arsip ZIP yang berisi *file* ".url" dengan nama seperti "B123456789012.url". Sekali lagi, ini tampaknya angka acak yang ditunjukkan pada Gambar 1.2.



Gambar 1.2 Contoh email dari 5 Maret 2018, kampanye FlawedAmmyy

Sumber: (Proofpoint Staff, 2018)

```
[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,9
[InternetShortcut]
IDList=
URL=file://buyviagraoverthecounterusabb.net/documents/B123177432431.js
HotKey=0
IconIndex=3
IconFile=C:\Windows\System32\shell32.dll
```

Gambar 1.3 isi *file* .url

Sumber (Proofpoint Staff, 2018)

Berkas .url diinterpretasikan oleh *Microsoft Windows* sebagai *file* "Internet Shortcut", contohnya dapat ditemukan di folder "Favorit" pada sistem operasi *Windows*. Jenis *file* ini dapat dibuat secara manual, ini dimaksudkan untuk melayani sebagai tautan ke situs internet, *launching default browser* secara otomatis, namun dalam hal ini penyerang menetapkan URL sebagai "*file*: //" berbagi jaringan, bukan http: // tautan biasa. Akibatnya, sistem mengunduh dan mengeksekusi *file JavaScript*

melalui protokol SMB daripada meluncurkan *browser* web jika pengguna mengklik "Buka" pada dialog peringatan yang ditunjukkan pada Gambar 1.4.

Gambar 1.4 Dialog peringatan ditampilkan setelah mengklik dua kali *file* .url

Sumber: (Proofpoint Staff, 2018)

JavaScript ini kemudian mengunduh *Quant Loader*, yang, dalam hal ini, mengambil RAT *Flawed Ammyy* sebagai payload akhir. Penggunaan *file* ".url" dan unduhan protokol SMB tidak biasa, dan ini adalah pertama kalinya para analis Proofpoint melihat metode ini digabungkan.

Flawed Ammyy RAT sebelumnya muncul pada tanggal 1 Maret dalam serangan yang ditargetkan secara sempit. Email berisi lampiran 0103_022.doc (Gambar 1.5), yang menggunakan makro untuk mengunduh RAT FlawedAmmyy secara langsung. Sampel ini menggunakan alamat perintah dan kontrol (C & C) yang sama dengan sampel dari kampanye besar-besaran pada 5 Maret.

Gambar 1.5 Screenshot dari lampiran dokumen dari 1 Maret 2018, kampanye *Flawed Ammyy*

Sumber: (Proofpoint Staff, 2018)

Analisa malware dengan menggunakan *Reverse Engineering* merupakan salah satu solusi yang bisa digunakan saat ini. *Reverse Engineering* digunakan pada dunia keamanan untuk mencari sebuah informasi yang tidak diketahui atau disembunyikan. Informasi yang didapat merupakan sebuah celah dari sistem pertahanan, sedangkan *Reverse Engineering* dalam analisis malware berguna untuk ekstraksi data yang memuat informasi yang ada didalam malware. (Nugroho & Prayudi, 2015)

Berdasarkan latar belakang yang telah dipaparkan sebelumnya, maka tugas akhir ini berjudul **"Analisis *Malware* "*Flawed Ammyy RAT*" Dengan Metode *Reverse Engineering*".**

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas maka rumusan masalah yaitu:

a. Bagaimana proses identifikasi serangan *Malware Flawed Ammyy RAT* menggunakan metode analisis dinamis dan *reverse engineering malware* dan hasil dari proses identifikasi malware Flawed Ammyy RAT dengan metode analisis dinamis dan reverse engineering?
b. Bagaimana cara kerja *Malware Flawed Ammyy RAT?*

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah diatas maka tujuan penelitian yaitu:

a. Mengetahui proses identifikasi serangan *Malware Flawed Ammyy RAT* menggunakan metode analisis dinamis dan *reverse engineering malware* dan melakukan dokumentasi hasil dari proses identifikasi malware Flawed Ammyy RAT dengan metode analisis dinamis dan reverse engineering.
b. Mengetahui cara kerja *Malware Flawed Ammyy RAT*

1.4 Batasan Masalah

Adapun batasan masalah dari penelitian yaitu:

a. *Malware* yang diteliti terfokus pada *malware "Flawed Ammyy RAT"*
b. Analisis yang dilakukan merupakan basic analisis
c. Penelitian yang dilakukan dalam *Virtual* mode
d. Penelitian dilakukan pada sistem oprasi *windows* 7
e. Aplikasi yang digunakan untuk analisis berbasis *freeware*

1.5 Manfaat penelitian

Manfaat dari penelitian ini yaitu agar hasil dari penelitian dapat dimanfaatkan dan digunakan oleh sebagai berikut:

a. Bagi Ilmu Pengetahuan
    1. Menambah wawasan tentang pola kerja *malware* khususnya *malware Flawed Ammyy RAT*
    2. Mengetahui proses identifikasi *malware Flawed Ammyy RAT*

b. Bagi Masyarakat Umum
    1. Mengetahui tanda-tanda sistem terserang *malware Flawed Ammyy RAT*
    2. Mengetahui cara pencegahan *malware Flawed Ammyy RAT*
    3. Mengetahui proses recovery sistem dari serangan *malware Flawed Ammyy RAT*

1.6 Metodologi

Metode penelitian menjelaskan mengenai tahapan atau prosedur penelitian untuk menganalisa suatu *malware* komputer, *malware* yang ada di lakukan analisis dengan melakukan analisis dinamis dan *Reverse Engineering* dengan kombinasi *tools* yang bersifat *freeware* dan dilakukan dalam lingkungan aman yaitu pengujian dalam model *virtual*.

1.7 Sistematika Penulisan

Sistematika penulisan untuk memahami lebih jelas isi laporan, materi-materi yang tertera pada laporan skripsi ini dikelompokkan menjadi beberapa sub bab dengan sistematika penyampaian sebagai berikut:

BAB I PENDAHULUAN

Berisi tentang latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisikan kajian dari penelitian terdahulu dan teori yang berupa pengertian dan definisi yang diambil dari kutipan jurnal, web, atupun buku serta beberapa literature *review* yang berkaitan dengan penyusunan laporan skripsi ini.

BAB III METODOLOGI PENELITIAN

Bab ini berisikan metodologi penelitian yang memberikan gambaran dan alur dari peneliian yang dilakukan, menjelaskan dari metodologi penelitian, kajian teori, analisis dinamis, analisis dinamis lanjut dan prosedur analisis data.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan hasil analisa *malware* dan pembahasan yang diusulkan dan yang di implementasikan, pembahasan secara detail mengenai analisis *malware flawed ammyy* menggunakan analisis dinamis.

BAB V SIMPULAN DAN HASIL

Bab ini berisi kesimpulan dan saran yang berkaitan dengan analisa berdasarkan yang telah diuraikan pada bab-bab sebelumnya.