BAB 2
DASAR TEORI DAN TINJAUAN PUSTAKA

Pada bab 2 akan dibahas tentang dasar teori yang digunakan dalam pembuatan Proyek Akhir ini.

2.1 Dasar Teori

2.1.1 Email Phising

Email Phising secara sederhana dapat diartikan sebagai sebuah penipuan dengan memanfaatkan akun untuk menguak informasi sensitif korban. Aksi phising dirancang mirip dengan lembaga atau institusi resmi agar korban percaya dengan tipuan pelaku.

2.1.2 *Malware*

Malware adalah software yang dibuat dengan tujuan memasuki dan terkadang merusak sistem komputer, jaringan, atau server tanpa diketahui oleh pemiliknya. Dalam analisis *Malware* yang dikirimkan melalui email phising dibutuhkan beberapa data penting seperti alamat email pengirim, sumber ip address, domain, file lampiran, data penting lainnya pada email header dan email body. Pada tahap analisi dapat menggunakan tools talos intelligent, virus total, urlscan, hybird analyst, dan any run. Website tersebut akan mengunakan sejumlah vendor virus untuk menggolongkan IP address, domain atau file tergolong dalam malicious.

2.1.3 Jenis-jenis *Malware*

Malware dikategorikan dalam beberapa jenis antaralain :

a. Trojan Horse

Malware ini dapat menyesatkan pengguna dengan cara berpura-pura menjadi program yang sah atau valid. Cara kerja *Malware* ini dengan menyebarkan rekayasa sosial seperti pishing dengan mengatasnamakan suatu perusahaan atau organisasi sehinga pengguna mengeksekusi email yang terdapat lampiran sehingga *Malware* dapat menyusup ke dalam sistem pengguna.

b. Rootkit

Rootkit adalah kumpulan *Malware* yang dirancang untuk memberikan akses tidak sah ke komputer atau area perangkat lunaknya dan sering kali menutupi keberadaannya atau keberadaan perangkat lunak lain. Instalasi rootkit dapat dilakukan secara otomatis atau penyerang dapat menginstalnya dengan akses administrator. Akses dapat diperoleh melalui serangan langsung pada sistem, seperti mengeksploitasi kerentanan, meretas kata sandi, atau phishing.

c. Ransomware

Ransomware adalah bentuk *Malware*, yang dirancang untuk menolak akses ke sistem komputer atau data hingga tebusan dibayarkan. Jenis *Malware* ini akan menyebar melalui email phishing, malvertising, mengunjungi situs web yang terinfeksi atau dengan mengeksploitasi kerentanan.

d. Adware

Adware adalah jenis grayware yang dirancang untuk memasang iklan di layar Anda, sering kali ditemukan di browser web atau popup. Biasanya jenis *Malware* ini akan membedakan dirinya sebagai sah atau mendukung program lain untuk mengelabui pengguna agar menginstalnya di komputer, tablet, atau ponsel cerdas mereka.

e. Spyware

Spyware yang mampu mengumpulkan informasi tentang seseorang atau perusahan, terkadang tanpa sepengetahuan mereka, dan mengirimkan informasi tersebut ke penyerang tanpa persetujuan korban.

2.1.4 Penggunaan Analisis *Malware*

Dalam analisis *Malware* terdapat dua jenis yaitu analisis secara static dan analisis secara dinamis.

a. Analisis static

Static analysis dilakukan dengan melakukan analisa kode program *Malware*, analisa gambar, string, dan resource disk lainnya. Teknik yang dilakukan adalah reverse engineering.

b. Analisis dinamis

Dynamic analisis merupakan analisa dengan menjalankan sampel *Malware* pada sebuah sandbox kemudian dilakukan analisis perilaku *Malware* dengan tujuan pengamatan adalah untuk memahami cara kerja *Malware*. Sandbox adalah analisis *Malware* dengan menggunakan mekanisme sandboxing yaitu menjalankan file *Malware* pada ruang lingkup yang terisolasi dari jaringan luar. Dari hasil analisis tersebut akan didapatkan informasi mengenai *Malware* dan perilakunya tanpa resiko infeksi *Malware* menyebar ke jaringan luar.

2.2 Tinjauan Pustaka

Pada penelitian sebelumnya, yang dilakukan oleh (Sulhaedir dan Febri Nova Lenti, 2016) yang berjudul “ANALISIS MALWAE TROJAN” adapun permasalahan pada penelitian ini yaitu, saat ini sangat banyak perangkat lunak yang ditawarkan secara gratis (freeware). Perangkat lunak freeware biasanya dapat didownload secara gratis memiliki banyak resiko seperti perangkat lunak sengaja dibuat lalu diberikan secara gratis tetapi perangkat lunak tersebut adalah sebuah *Malware* dengan jenis perangkat lunak yang dikembangkan dengan tujuan kejahatan. Pada Penelitian diatas, dapat disampaikan bahwa penelitian sebelumnya dilakukan analisis dengan metode dinamis. Dalam hal ini saya akan membuat implementasi pada analisis *Malware* jenis Trojan.