BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam perkembangannya, teknologi selalu mengalami pembaharuan dan selalu memiliki tantangan dari setiap hal baru yang ada. Pengembangan yang dilakukan ini selain mempunyai dampak positif juga memiliki dampak negatif, diantaranya merambahnya tindak kejahatan yang awalnya berada di dunia nyata, kini sudah ada di dunia maya atau sering kita sebut dengan *cyber crime*, dimana *cybercrime* saat ini sudah semakin banyak, mulai dari berbagai macam jenis serangan, tingkat penyebaran serangan yang terjadi, hingga kerugian yang ditimbulkan akibat dari serangan para pelaku *cybercrime* ini. Tindak kejahatan ini bisa dilakukan lintas Negara dan menimbulkan kerugian yang bermacam-macam, mulai dari kehilangan file, pengambilan data informasi secara diam-diam dan lain sebagainya. Secara umum tindak kejahatan ini dilakukan mengarah pada *system computer* dimana serangan yang dilakukan menggunakan komputer sebagai alat bantu dalam melakukan serangan terhadap target. Kejahatan yang dilakukan di dunia maya tidak melukai secara fisik dan juga peraturan yang mengatur tentang perlindungan terhadap serangan *cyberspace* sering disebut dengan istilah *cybercrime law*, dan serangan yang dilakukan disebut *cybercrime*, sedangkan pelaku dari serangan sering disebut dengan nama *cybercriminal*.[1]

Pelaku dari tindak kejahatan dunia maya yang memanfaatkan bidang teknologi informasi sering disebut dengan *cybercriminal* dimana pelaku dapat dilihat dari keterlibatannya dalam melakukan serangan serta peran yang dilakukan guna memperlancar tindak pidana tersebut, sehingga dari tindakannya tersebut dapat dilakukan pertanggungjawaban secara pidana sesuai ketentuan dari *cybercrime law* dari masing-masing Negara, karena tindak kejahatan ini bisa dilakukan lintas Negara atau secara jarak jauh. Setiap tindak kejahatan yang terjadi di dunia maya dapat terjadi karena adanya celah dari sistem keamanan

yang sudah ada, selain dari sistem keamanan jaringan yang ada, serangan ini bisa terjadi karena tidak adanya kewaspadaan pengguna *cyberspace* terhadap setiap kegiatan yang dilakukan di dunia maya.

Gambar 1.1 Diagram serangan malware di Indonesia

(sumber : vaksin.com)

Pada diagram diatas diperlihatkan bahwa perkembangan serangan malware di Indonesia mengalami pentingkatan, yang seharusnya menjadi perhatian kita adalah serangan terkait Trojan, dimana kita bendaknya melakukan perlindungan terhadap serangan yang bisa menyerang pada perangkat yang kita gunakan seperti laptop, bahkan *smartphone*, yang saat ini bisa disisipi serangan berupa RAT *(Remote Access Trojan)*

RAT *(Remote Access Trojan)* adalah sebuah program malware yang sengaja dibuat untuk mendapatkan kontrol secara penuh dari sebuah sistem. Serangan malware RAT ini seringkali tidak terdeteksi oleh sistem, setelah kontrol penuh terhadap target didapatkan mereka dapat melakukan serangan terhadap perangkat lain tanpa diketahui bahwa hal yang dilakukan tersebut berbahaya. Dimana RAT yang ada pada smartphone bisa melakukan akses find location, call phone, camera, record audio, dan lain-lain. [2]

Malware RAT yang sudah berkembang dapat menyerang para pengguna smartphone terkhusus android, dimana serangan dari malware RAT pada android ini dapat dengan mudah masuk melalui proses unduh yang dilakukan oleh user pada saat menggunakan smartphone. Tingkat kewaspadaan para pengguna

smartphone terhadap serangan malware RAT terhadap android yang masih jarang dibahas dalam beberapa literature [3]. Analisis yang dilakukan pada penelitian ini dilakukan dengan menggunakan metode deskriptif kuantitatif dimana nantinya hasil dari penelitian yang berupa angka akan di bahasakan sehingga menjadi lebih mudah dalam memahami hasil akhir dari penelitian ini.

Pada latar belakang yang sudah dipaparkan diatas maka ranah dari penelitian ini adalah melakukan analisis tingkat kewaspadaan siswa terhadap ancaman malware RAT pada smartphone android dengan menggunakan metode deskriptif kuantitatif serta melibatkan 30 siswa SMA N 1 Sentolo yang tergabung dalam OSIS untuk menjadi responden dalam penelitian ini. Untuk hasil dari penelitian ini semoga memberikan pengetahuan siswa terkait pentingnya menjaga keamanan dari smartphone yang mereka gunakan, karena pada masa pandemi dan sekolah menggunakan metode daring siswa akan lebih banyak mengakses internet untuk melakukan aktivitas belajar.

1.2 Rumusan Masalah dan Hipotesis

Berdasarkan latar belakang yang ada, maka rumusan masalah dari penelitian ini adalah seberapa besar presentase tingkat kewaspadaan siswa dan siswi di SMA N 1 Sentolo terkait ancaman yang dapat ditimbulkan oleh *malware RAT (Remote Access Trojan).*

1.3 Batasan Masalah

Untuk mengerucutkan permasalahan yang akan diangkat pada skripsi ini diberikan batasan-batasan masalah sebagai berikut :

a. Penelitian ini menggunakan serangan malware RAT *(Remote Access Trojan)* sebagai inti permasalahan yang diangkat.
b. Menggunakan metode deskriptif kuantitatif dalam melakukan pengambilan data dari responden
c. Responden yang digunakan adalah siswa-siswi yang menggunakan *smartphone android*

d. Pengambilan data kuesioiner menggunakan google form yang nantinya akan diisi oleh responden.

1.4 Tujuan Penelitian

Tujuan dari penulisan laporan skripsi ini adalah mendapatkan presentase terkait tingkat kewaspadaan siswa dan siswi di SMA N 1 Sentolo terkait ancaman yang dapat ditimbulkan akibat serangan dari *malware RAT (Remote Access Trojan)* sehingga dapat dijadikan acuan guna peningkatan pengetahuan terhadap ancaman yang dapat terjadi akibat *malware RAT (Remote Access Trojan)*

1.5 Sistematika Penulisan

Pada bagian ini terdapat 5 bab yang dimana pada masing-masing bab memiliki peran dan bagian yang berbeda.

Bab I Pendahuluan yang berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan.

Bab II Landasan Teori berisi Tinjauan Pustaka, serta refrensi terkait jurnal maupun laporan skripsi yang sejenis, penjelasan tentang apa itu RAT, serta seberapa berbahayanya serangan RAT yang bisa terjadi ataupun menyerang smartphone kita.

Bab III Metedologi Penelitian berisi tentang : Deskripsi singkat dari Objek, analisis permasalahan, solusi yang ditawarkan, Alat dan bahan penelitian, dan metode penelitian, dimana pada bagian ini secara sistematis terkait penelitian yang dilakukan.

Bab IV Pembahasan berisi : pengolahan data hasil dari penelitian, penerapan metode penelitian yang digunakan, melakukan penghitungan hasil dari kuesioner, mengelola hasil untuk dijadikan hasil dari penelitian dengan menghitung masing-masing persentase yang terdapat pada setiap variabel.

Bab V Penutup berisi tentang : kesimpulan dari penelitian serta hasil akhir yang ingin disampaikan sesuai dengan hasil dari penelitian yang sudah dilakukan maupun pengolahan data yang ada pada objek dalam hal ini adalah siswa SMA N 1 Sentolo terkait tingkat kewaspadaan siswa terhadap serangan malware RAT yang dapat menyerang android.