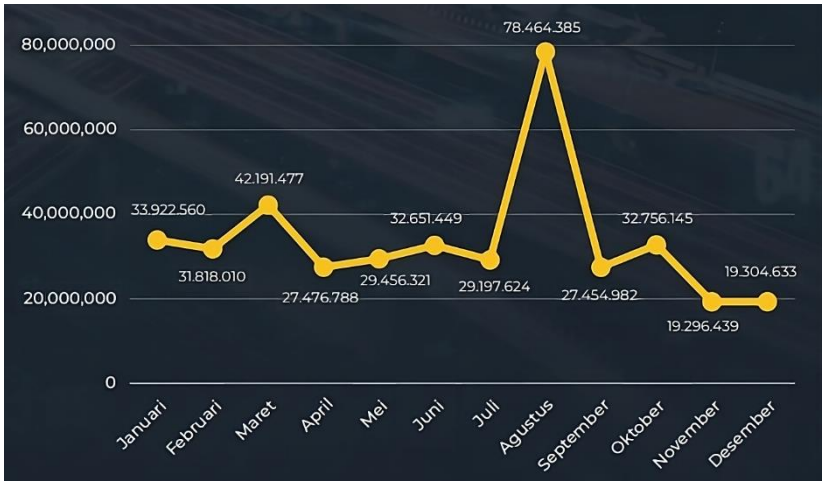
BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Keamanan adalah kebutuhan dasar manusia, di mana manusia selalu berusaha menciptakan lingkungan yang aman untuk melindungi diri dari ancaman. Pada era digital saat ini, teknologi telah menjadi bagian integral dari kehidupan sehari-hari, yang memfasilitasi berbagai aktivitas. Dengan semakin meningkatnya ketergantungan terhadap teknologi, kebutuhan akan pengamanan digital menjadi semakin mendesak. Pengamanan aset digital sangat penting untuk dilakukan (Syafuddin, 2023). Aset digital ini mencakup segala sesuatu yang bisa disimpan dalam format digital dan memiliki nilai (Cicala & Bertino, 2022). Aset digital ini meliputi berbagai hal, seperti data pribadi, informasi keuangan, dokumen penting, konten multimedia, surat elektronik, situs web, berbagai bentuk mata uang digital, infrastruktur IT seperti perangkat lunak, dan masih banyak lagi. Mengingat nilai strategis dari aset-aset digital ini, mereka sering menjadi target serangan siber. Untuk merespon kebutuhan ini, berbagai teknologi dan prinsip dasar keamanan siber telah dikembangkan untuk memastikan perlindungan yang efektif terhadap aset digital. Salah satu prinsip dasar yang sering diterapkan adalah konsep CIA, yang terdiri dari *Confidentiality* (Kerahasiaan), *Integrity* (Integritas), dan *Availability* (Ketersediaan). Konsep CIA ini menjadi pondasi bagi banyak kebijakan dan praktik keamanan. *Confidentiality* bertujuan untuk memastikan bahwa data hanya dapat diakses oleh pihak yang berwenang; *Integrity* menjamin bahwa data tetap tidak berubah tanpa izin; dan *Availability* memastikan bahwa data serta sistem tetap dapat diakses oleh pengguna yang sah. Di Indonesia, framework NIST (*National Institute of Standards and Technology*) adalah salah satu panduan yang digunakan untuk melindungi aset digital, dengan pedoman yang mencakup manajemen risiko, pengendalian akses, dan respons terhadap insiden secara menyeluruh. Standar NIST membantu dalam meminimalkan risiko ancaman digital. Pengamanan aset digital tidak hanya bergantung pada teknologi, tetapi juga pada kesadaran dan edukasi pengguna. Keamanan digital harus mencakup sistem yang kuat dan pengguna yang teredukasi.

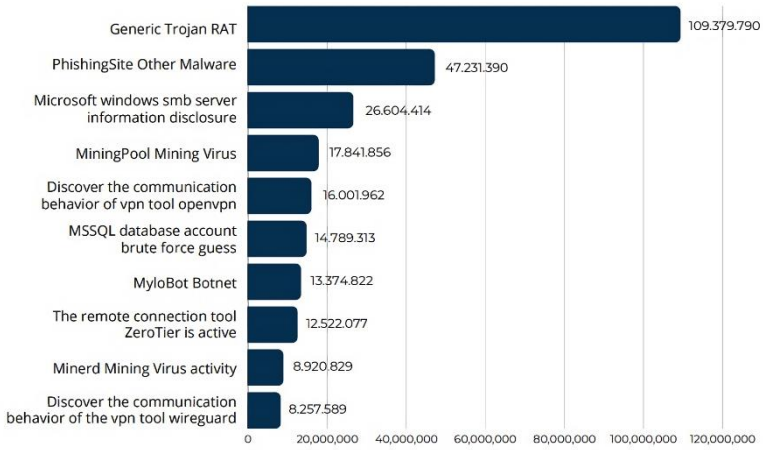
Berdasarkan laporan *Global Cybersecurity Index* (GCI) (dalam Cloramidine & Badaruddin, 2023), yang dirilis oleh *The International Telecommunication Union* (ITU) PBB tahun 2021, Indonesia berada pada peringkat ke-24 dari 194 negara dan mengalami peningkatan dari peringkat ke-41 di tahun 2018. Kondisi ini menunjukkan bahwa keamanan siber di Indonesia masih lemah dan perlu dioptimalkan. Pemerintah Indonesia memberikan perhatian khusus terhadap masalah keamanan siber dengan membentuk Badan Siber dan Sandi Negara (BSSN) untuk menjaga keamanan dan kedaulatan siber. Selain itu, pemerintah juga aktif dalam mendorong isu keamanan siber di tingkat bilateral dan multilateral (Chotimah, 2019). Dilansir dari (Badan Siber dan Sandi Negara, 2023) total trafik anomali di Indonesia pada tahun 2023 mencapai 403.990.813. Jumlah anomali tertinggi adalah bulan Agustus dengan 78.464.385 anomali, sedangkan jumlah terendah terjadi pada bulan November dengan 19.296.439 anomali. Aktivitas trafik anomali ini dapat mengakibatkan penurunan performa perangkat dan jaringan, pencurian data sensitif, serta merusak reputasi dan menurunkan kepercayaan terhadap organisasi. Berikut adalah grafik trafik anomali dari Januari hingga Desember 2023.



Gambar 1.1 Grafik Trafik Anomali Januari - Desember 2023

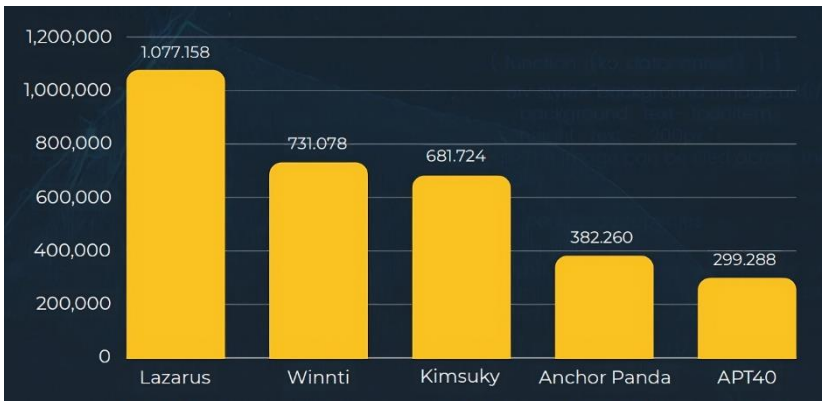
Gambar 1.1 adalah sebuah grafik garis yang menggambarkan jumlah atau frekuensi anomali trafik yang terjadi setiap bulan dalam satu tahun. Grafik ini secara umum menunjukkan fluktuasi dalam jumlah anomali trafik sepanjang tahun, dengan lonjakan besar pada bulan Agustus dan penurunan bertahap setelahnya.

Berdasarkan grafik trafik anomali tahun 2023 terdapat top 10 kasus yang terjadi. Berikut merupakan gambar diagram Top 10 Traffic Anomali Tahun 2023 berdasarkan Badan Siber dan Sandi Negara (BSSN).



Gambar 1.2 Top 10 Trafik Anomali Tahun 2023

Gambar 1.2 menunjukkan distribusi dari 10 serangan siber yang paling sering terjadi di Indonesia. Generic *Trojan RAT* menduduki peringkat teratas dengan jumlah kasus yang sangat tinggi dibandingkan dengan jenis serangan lainnya. *Generic Trojan RAT*, *PhishingSite Other Malware*, *Microsoft Windows SMB Server Information Disclosure*, *MiningPool Mining Virus*, *Discover the Communication Behavior of VPN Tool OpenVPN* dan *Minerd Mining Virus Activity* jika diklasifikasikan masuk ke dalam kejahatan siber jenis *malware*. Kemudian *MSSQL Database Account Brute Force Guess* termasuk ke dalam jenis kejahatan siber *Brute Force Attack*. Sedangkan *MyloBot Botnet* merupakan kejahatan siber jenis *Botnet*.



Gambar 1.3 Aktivitas *Ransomware* yang terjadi di Indonesia Tahun 2023

Pada tahun 2023 juga terdapat 1.011.209 Aktivitas *Ransomware* yang terjadi di Indonesia. Gambar 1.3 menunjukkan 5 *ransomware* yang paling banyak ditemukan pada ruang siber Indonesia berdasarkan hasil monitoring trafik anomali. *Luna Moth* menduduki peringkat teratas dengan jumlah aktivitas sangat tinggi dibandingkan dengan jenis *ransomware* lainnya.

Gambar 1.4 Contoh Kasus Serangan *Ransomware*

Dilansir dari berita CNN Indonesia (Kertopati, 2017) Gambar 1.4 merupakan contoh konkret, pada tahun 2017 dimana Indonesia mengalami insiden yang menyebabkan kerugian materi dan ekonomi yang tidak sedikit, yaitu serangan *ransomware WannaCry* yang menyerang Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais di Jakarta. *Malware* ini menyerang ratusan server dan komputer, yang mengakibatkan terganggunya operasional rumah sakit. Kejadian ini menyoroti kelemahan dalam infrastruktur keamanan siber dan perlunya peningkatan dalam deteksi serta respons terhadap ancaman siber.

Serangan siber yang tercermin dalam top 10 trafik anomali di Indonesia pada tahun 2023 dan kasus yang dilansir dalam CNN dapat terjadi karena kelalaian pengguna dalam menjaga keamanan digital mereka. Masalah utama yang dihadapi adalah rendahnya kesadaran dan pemahaman masyarakat terhadap ancaman siber dan cara untuk menghadapinya. Hal ini disebabkan oleh edukasi siber yang belum terpenuhi dengan baik. Dalam banyak kasus, masyarakat tidak menyadari bahwa mereka menjadi target serangan siber. Rendahnya kesadaran ini berkontribusi pada

peningkatan jumlah serangan yang berhasil, terutama dalam bentuk serangan *malware* salah satunya yaitu *ransomware* yang terus berkembang. Serangan *ransomware* dapat menyebabkan kerugian besar, baik dari segi materi maupun operasional. Serangan *ransomware* telah menjadi ancaman global yang terus berkembang dengan dampak yang sangat merugikan bagi individu, organisasi, dan institusi. *Ransomware* memiliki kemampuan untuk menyebar dengan cepat dan menyerang sistem yang rentan, yang mengakibatkan gangguan besar dalam operasi sehari-hari. Namun serangan siber ini juga terjadi bukan hanya disebabkan karena kelalaian pengguna saja melainkan dapat disebabkan oleh kelemahan dalam infrastruktur sistem, kerentanan perangkat lunak, serta kurangnya deteksi dan respons yang cepat terhadap ancaman siber. Oleh karena itu sangat penting untuk menumbuhkan *cybersecurity culture* sehingga masyarakat luas memiliki kesadaran terkait resiko ancaman dan serangan siber (Islami, 2017)

Salah satu pendekatan yang efektif untuk menumbuhkan kesadaran keamanan siber ini adalah melalui metode "*learning by doing*", di mana individu belajar dengan cara mengalami langsung situasi yang mensimulasikan ancaman nyata. Dalam konteks keamanan siber, pendekatan ini dapat diwujudkan melalui *game* berbasis komputer (*computer-based learning*). Aplikasi ini memanfaatkan gamifikasi untuk meningkatkan kesadaran dan pemahaman masyarakat terhadap serangan siber melalui pengalaman langsung yang menantang dan menghibur. Inovasinya terletak pada kemampuannya mensimulasikan situasi serangan nyata, memungkinkan pengguna belajar melalui praktik dan pengalaman. Maka dari itu, Penelitian ini bertujuan untuk merancang dan mengembangkan aplikasi "*RansomForge*" yang didasarkan pada hasil analisis dekompilasi *ransomware* sebagai alat edukasi dalam meningkatkan kesadaran dan pemahaman masyarakat terhadap ancaman siber, khususnya serangan *ransomware*. Diharapkan aplikasi ini dapat meningkatkan kesadaran masyarakat terhadap keamanan siber dengan cara yang lebih menarik dan interaktif.

1.2 Rumusan dan Batasan Masalah Penelitian

1.2.1 Rumusan Masalah

Berdasarkan latar belakang penelitian, terdapat rumusan masalah sebagai berikut:

1. Bagaimana mekanisme dan cara kerja *ransomware* berdasarkan hasil analisis dekompilasi?
2. Bagaimana hasil rancang bangun aplikasi *RansomForge* berdasarkan hasil analisis dekompilasi *ransomware*?

1.2.2 Batasan Masalah

Untuk memastikan penelitian ini tetap fokus dan terarah, beberapa batasan telah ditetapkan. Adapun batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Penelitian ini dibatasi pada *ransomware* yang spesifik, yaitu yang didistribusikan dalam format .exe dengan jenis *Crypto Ransomware/Encrypting Ransomware*, sehingga hasil yang diperoleh hanya berlaku untuk tipe *ransomware* ini dan tidak mencakup varian lain yang mungkin memiliki karakteristik berbeda.
2. Batasan penelitian ini mencakup hanya pada aspek teknis dari analisis dekompilasi *ransomware*, yang melibatkan pembongkaran kode *ransomware*, analisis fungsi, dan pemahaman struktur kode, tanpa membahas dampak sosial, psikologis, atau ekonomi dari serangan *ransomware*.
3. Rancang bangun aplikasi *game RansomForge* didasarkan pada temuan hasil analisis dekompilasi *ransomware* tersebut, dengan fokus pada pembuatan elemen simulasi dan edukasi untuk meningkatkan kesadaran akan keamanan siber. Pengembangan aplikasi ini dibatasi pada tahap pengujian dengan menggunakan *Black Box Testing* dan tahap pengujiannya hanya sampai pengujian alpha dan beta saja, tanpa masuk ke tahap penyebaran atau implementasi skala besar.
4. Pengembangan aplikasi *game RansomForge* dibatasi pada platform *Android* dan menggunakan *Unity* sebagai *game engine*.

1.3 Tujuan Penelitian

Berdasarkan pada rumusan masalah diatas, berikut merupakan tujuan dari penelitian yang dilakukan:

1. Untuk menganalisis dan mengidentifikasi struktur serta mekanisme kerja *ransomware* melalui proses dekompilasi.
2. Untuk merancang dan mengembangkan aplikasi *game* bernama *RansomForge* yang didasarkan pada hasil analisis dekompilasi *ransomware*.

1.4 Manfaat / Signifikansi Penelitian

Penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. **Manfaat Teoritis**

   Penelitian ini memberikan kontribusi yang signifikan terhadap literatur dan teori dalam bidang keamanan siber, khususnya dalam memahami hasil analisis dekompilasi terkait pembuatan *ransomware*. Penelitian ini memperkaya pengetahuan yang ada tentang teknik dan proses pengembangan *ransomware* untuk pengembangan teori keamanan siber lebih lanjut. Selain itu, penelitian ini juga memperkenalkan model pembelajaran baru melalui *game* simulasi yang dapat menjadi referensi dalam pengembangan metode pendidikan keamanan siber.

2. **Manfaat Praktis**

   a. Meningkatkan kesadaran dan pengetahuan, aplikasi *game* simulasi yang dikembangkan diharapkan dapat digunakan untuk meningkatkan kesadaran dan pengetahuan tentang *ransomware* di kalangan pengguna baik individu maupun organisasi serta membantu pengguna dalam meminimalisir risiko dan menangani ancaman dengan lebih efektif.

   b. Alat edukasi yang efektif, aplikasi *game* simulasi ini diharapkan dapat berfungsi sebagai alat pelatihan yang interaktif dan praktis yang memungkinkan pengguna untuk belajar dan berlatih menghadapi *ransomware* tanpa risiko nyata.

   c. Memberikan kontribusi praktis dalam pengembangan materi pendidikan yang lebih efektif, serta menyediakan referensi bagi pengembangan metode pembelajaran interaktif lainnya di bidang keamanan siber.

d. Hasil penelitian ini dapat menjadi panduan bagi pengembang *game* edukasi lainnya yang ingin mengintegrasikan elemen keamanan siber ke dalam *game* mereka, baik dari segi desain, alur permainan, maupun metode pengujian untuk memastikan efektivitasnya.

1.5 Struktur Organisasi Skripsi

Struktur organisasi skripsi memberikan gambaran tentang sistematika penulisan pada setiap babnya. Skripsi ini terdiri dari lima bab, yaitu: pendahuluan; tinjauan pustaka; metode penelitian; temuan dan pembahasan; serta simpulan, implikasi, dan rekomendasi, yang dijelaskan secara rinci sebagai berikut:

1. BAB I PENDAHULUAN

   Pada bab I dalam penelitian ini mencakup latar belakang penelitian, rumusan dan batasan masalah, tujuan penelitian, manfaat penelitian dan struktur organisasi skripsi.

2. BAB II KAJIAN PUSTAKA

   Pada bab II dalam penelitian ini berisi kajian literatur, memaparkan teori-teori yang relevan dengan topik penelitian ini. Topik yang dibahas meliputi *cyber security* (keamanan siber), *ransomware*, *computer based learning*, *game*, dan hasil-hasil penelitian yang relevan.

3. BAB III METODE PENELITIAN

   Pada bab III dalam penelitian ini menguraikan metode penelitian yang digunakan, termasuk jenis penelitian, prosedur penelitian, subjek penelitian, instrumen penelitian, dan teknik analisis data.

4. BAB IV TEMUAN DAN PEMBAHASAN

   Pada bab IV dalam penelitian ini memaparkan temuan-temuan berupa hasil yang diperoleh dari penelitian secara rinci, diikuti dengan pembahasan yang mendalam untuk menjelaskan makna dari temuan tersebut.

5. BAB V SIMPULAN, IMPLIKASI, DAN REKOMENDASI

   Pada bab V dalam penelitian ini berisi kesimpulan yang diambil dari hasil penelitian dan pembahasan pada bab sebelumnya. Bab ini juga mencakup implikasi dari temuan penelitian, yang menjelaskan bagaimana hasil penelitian dapat diterapkan dalam konteks praktis atau teoritis. Terakhir, bab ini

memberikan rekomendasi untuk penelitian lebih lanjut atau tindakan yang dapat diambil berdasarkan temuan penelitian.