BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan di dunia *IT* telah mengubah dunia secara drastis. Inovasi yang cepat dalam komputer, telekomunikasi, dan internet telah menghubungkan orang-orang di seluruh dunia. Peralatan pintar, seperti *smartphone*, telah menjadi bagian tak terpisahkan dari kehidupan sehari-hari. *Internet of Things* (IoT) memungkinkan pengendalian perangkat melalui jaringan, sementara kecerdasan buatan (AI) mendorong kemajuan di bidang seperti otomatisasi, pengenalan suara, dan analisis data yang canggih. Teknologi baru seperti *realitas virtual* (VR) dan *augmented reality* (AR) memberikan pengalaman yang mendalam dan imersif. Namun, perkembangan ini juga memunculkan tantangan baru dalam hal privasi data, keamanan siber, dan kesenjangan teknologi.

Dengan pesatnya perkembangan teknologi keamanan siber pun menjadi tantangan dan masalah baru pada saat ini. Keamanan jaringan melawan *malware* menjadi penting dalam menghadapi ancaman yang terus berkembang di dunia digital saat ini. *Malware*, singkatan dari *malicious software*, merujuk pada perangkat lunak berbahaya yang dirancang untuk merusak atau mencuri data pengguna tanpa izin. Serangan *malware* dapat mengakibatkan kerugian finansial, kehilangan data berharga, atau bahkan merusak reputasi perusahaan. Organisasi dan pengguna perlu mengadopsi langkah-langkah keamanan yang tepat untuk

melindungi jaringan mereka. Ini melibatkan penggunaan perangkat lunak antivirus yang *up-to-date*, *firewall* yang kuat, pendidikan dan kesadaran pengguna, pembaruan sistem secara teratur, dan kebijakan keamanan yang ketat. Upaya yang berkelanjutan diperlukan untuk menghadapi ancaman *malware* yang terus berkembang dan menjaga integritas jaringan.

Perusahaan swasta dan instansi lain sudah mulai mengambil langkah strategis tentang kemanan jaringan dan data pada perusahan mereka. Salah satunya PT Nok Precision Component Batam (PT. NPCB) merupakan salah satu perusahaan yang bergerak dalam bidang produksi dan pengelolaan *Hard Disk*, *Drive*, *Top Cover* yang terletak diwilayah Muka Kuning Batam. Seiring dengan perkembangan teknologi, PT Nok Precision Component Batam juga mengalami perkembangan yang cukup pesat dengan penggunaan sistem yang terkomputerisasi. Perkembangan teknologi yang canggih, proses pengiriman data tidak bias terlepas dari penggunaan jaringan komputer, karena penggunaan jaringan komputer dalam pengiriman data yang efisien dan efektif.

Setiap komputer yang terhubung dengan jaringan komputer memiliki resiko akan terkenanya serangan *malware*, begitu juga dengan komputer-komputer yang ada di PT Nok Precision Component Batam. Karena itu, untuk efisien dan harusnya pembagian data serta pengiriman data, maka setiap komputer yang terhubung dengan jaringan komputer. Sehingga menyebabkan mudahnya serangan malware yang terjadi di komputer-komputer yang terhubung dalam jaringan tersebut.

Malware merupakan perangkat lunak yang digunakan untuk meretas atau merusak sistem didalam komputer. Saat ini penyebaran *malware* sangat mudah,

baik melalui flashdisk, iklan pada *website*, dan media lainnya. Hal itulah yang menyebabkan tindakan kejahatan seperti pencurian data, internet banking, kartu kredit, dan lain sebagainnya. Oleh karena itu, ada suatu bidang yang menangani tindakan kejahatan itu, yaitu forensik digital. Salah satu tahapannya yaitu melakukan analisis terhadap barang bukti digital, dalam hal ini adalah *malware*. Banyak ragam dari *malware* yaitu *Virus, Trojan, Worm, Adware, Spyware, Ransomware, Rootkit, Keylogger, Botnet, Fileless Malware*. Yang saat ini sangat popular adalah serangan *Ransomware*. *Ransomware* adalah jenis khusus *malware* yang bertujuan untuk mengunci atau mengenkripsi data pada sistem komputer yang terinfeksi. Setelah data terkunci, penyerang meminta pembayaran tebusan (*ransom*) dari korban agar mereka dapat mendapatkan kunci dekripsi untuk mengembalikan akses ke data mereka (Manoppo et al., 2020).

Ransomware dapat menyebar melalui metode yang sama seperti *malware* lainnya, seperti melalui email phishing, situs *web* yang terinfeksi, atau eksploitasi kerentanan dalam sistem operasi atau perangkat lunak. Setelah ransomware mengenkripsi data, korban sering diberi tahu melalui pesan tebusan yang menuntut pembayaran dalam bentuk mata uang digital, seperti *Bitcoin*.

Pembayaran tebusan tidak menjamin bahwa data akan dikembalikan, dan dalam beberapa kasus, bahkan setelah pembayaran, data mungkin tetap terenkripsi atau bahkan dihapus. *Ransomware* telah menjadi ancaman yang semakin serius, dengan serangan besar seperti itu yang menyebabkan kerugian finansial yang signifikan dan mengganggu operasi banyak organisasi di seluruh dunia.

Menurut (Wahidin et al., 2022) Indonesia menempati posisi ketiga di Asia Tenggara, dengan jumlah serangan *ransomware* terbanyak, sebesar 14 laporan serangan *ransomware*. Menurut catatan Palo Alto Networks, pelaku ancaman menggunakan taktik yang lebih agresif untuk menekan organisasi, dengan jumlah gangguan 20 kali lebih banyak dibandingkan 2021, menurut kasus penanganan insiden Unit 42. Temuan ini selaras dengan laporan Badan Siber dan Sandi Negara (BSSN), yang menyebut bahwa *ransomware* dan pembobolan merupakan jenis serangan siber paling umum di 2022. Menurut BSSN, mereka menyumbang 50 persen dari seluruh serangan siber yang dilaporkan di Indonesia pada tahun 2022 (Wahidin et al., 2022).

Gangguan ini biasanya dilakukan lewat panggilan telepon dan email yang menargetkan individu tertentu, seringkali di *C-suite* atau pelanggan, untuk mendesak agar membayar permintaan uang tebusan. Untuk melindungi diri dari *malware* dan *ransomware*, penting untuk menjaga sistem operasi dan perangkat lunak yang terinstal tetap diperbarui, menggunakan solusi keamanan yang terkini, waspada terhadap *email* yang mencurigakan atau tautan yang tidak diketahui, serta melakukan pencadangan data secara teratur sebagai langkah pencegahan utama.

Analisa *malware* secara umum dapat dilakukan dengan dua metode, yaitu *Dynamic Analysis*, dan *Static Analysis*. Meskipun tujuan dari kedua metode tersebut sama yaitu untuk menjelaskan tentang bagaimana sebuah *malware* bekerja tetapi dalam proses analisa kedua metode tersebut sangatlah berbeda baik dari segi *tools*, waktu dan kemampuan. *Dynamic analysis* dilakukan dengan mengeksekusi contoh *malware* untuk kemudian dipelajari perilaku yang ditimbulkan oleh *malware*

tersebut. Berbeda pula dengan *static analysis* yang pada saat proses analisanya tidak mengeksekusi contoh *malware* melainkan dengan membongkar *source code malware* lalu mempelajari dan memahami kode tersebut (Manoppo et al., 2020)

Dynamic Analysis dapat dilakukan menggunakan dua cara yaitu manual dan atau menggunakan tool analisa otomatis yaitu *cuckoo sandbox. Cuckoo sandbox* dapat melakukan analisa *malware* secara otomatis dan menampilkan informasi-informasi yang dilakukan oleh sampel *malware*. *Cuckoo Sandbox* merupakan *tool* analisa *malware* dan dapat memberikan beberapa informasi mengenai *malware* yang sedang berjalan dalam lingkungan yang terisolasi (Manoppo et al., 2020).

Malware Analysis Static tidak sama dengan *Malware Analysis Dynamic*, dalam metode analisis statis ini file *malware* tidak akan diaktifkan secara langsung melainkan diteliti serta dianalisis terhadap kode sumber yang dituliskan didalam program *malware* dengan menggunakan tahapan pembedahan terhadap program *malware* tersebut, sehingga informasi yang didapatkan lengkap dan bisa memberikan gambaran detail tentang mekanisme kerja *malware* tersebut secara keseluruhan (Manoppo et al., 2020).

Berdasarkan dampak yang dapat disebabkan oleh *malware* jenis *Ransomware* bagi pengguna dan protokol jaringan komputer yang dapat menghambat kinerja PT Nok Precision Component Batam, maka peneliti termotivasi untuk melakukan penelitian yang berjudul **"ANALISIS DAN DETEKSI *MALWARE* PADA PROTOKOL JARINGAN MENGGUNAKAN METODE *MALWARE* ANALISIS DINAMIS DAN *MALWARE* ANALISIS STATIS".**

1.2 Identifikasi Masalah

Sesuai yang dijabarkannya latar belakang masalah, adapun identifikasi masalah pada penelitian ini yaitu:

1. Kesulitan melakukan mitigasi dan pencegahan *ransomware* yang mengenkripsi data pada sistem komputer yang terinfeksi, membuatnya tidak dapat diakses oleh pemiliknya. Ini dapat menyebabkan kerugian finansial dan operasional yang signifikan bagi organisasi, karena data yang terenkripsi mungkin berisi informasi penting, termasuk data pelanggan, data bisnis, atau data keuangan.
2. Kurangnya keamanan jaringan sehingga mudah untuk diserang dari infrastruktur dan tenanga khusus analis dan team kemana siber pada perusahaan.
3. Perkembangan yang cepat serta varian dari jenis *ransomware* yang selalu berkemangan dengan teknik yang berbeda beda dari tahun ke tahun.

1.3 Batasan Masalah

Berdasarkan identifikasi masalah diatas, dan penelitian ini tidak terlalu luas cakupannya maka peneliti hanya membatasi masalah sebagai berikut:

1. Perangkat yang digunakan adalah *virtual machine* dengan sistem operasi *windows* 7 yang dijalankan dengan *virtualbox*.
2. Analisis yang akan dilakukan adalah dasar analisis statis.
3. Analisis dinamis dilakukan menggunakan *cuckoo sandbox* dan akan menghasilkan data *behaviour* analisis dan *process tree*.
4. *Ransomware* yang akan dianalisis hanya jenis *Petya* dan *Gandcrab*.

1.4 Rumusan Masalah

Berdasarkan batasan masalah yang telah dijabarkan diatas, adapun rumusan masalah dari penelitian ini yaitu;

1. Bagaimana cara menyiapkan *environment* khusus untuk melihat jenis *Ransomware Petya* dan *Grandcrab*?
2. Bagaimana cara melakukan analisis statis dengan benar?
3. Bagaimana cara melakukan analisis dinamis menggunakan *Cuckoo Sandbox*?
4. Bagaimana melakukan mitigasi dan pemetaan evolusi dari kedua metode analisis tersebut?

1.5 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijabarkan diatas, adapun tujuan dari penelitian ini yaitu;

1. Untuk menyiapkan *environment* khusus untuk melihat jenis *Ransomware Petya* dan *Grandcrab*.
2. Untuk melakukan analisis statis dengan benar.
3. Untuk melakukan analisis dinamis menggunakan *Cuckoo Sandbox*.
4. Untuk melakukan mitigasi dan pemetaan evolusi dari kedua metode analisis tersebut.

1.6 Manfaat Penelitian

Hasil dari penelitian yang dilakukan penulis berharap kiranya dapat bermanfaat bagi berbagai pihak, adapun manfaat dari penelitian ini yaitu;

1.6.1 Manfaat Teoritis

Penulis berharap baik secara langsung maupun tidak langsung penelitian ini dapat bermanfaat pada berbagai pihak, yaitu diantaranya:

1. Menambah wawasan dalam bidang menganalisa jenis serangan *malware* khususnya *ransomware* jaringan menggunakan metode analisis statis dan dinamis.
2. Menambah keahlian dalam bidang menganalisa, mitigasi serangan ataupun ancaman *ransomware* pada jaringan menggunakan metode *malware* analisis statis dan dinamis.
3. Mengetahui keamanan jaringan yang dapat diserang orang yang tidak bertanggung jawab.

1.6.2 Manfaat Praktis

Penulis berharap baik secara langsung maupun tidak langsung penelitian ini dapat bermanfaat pada berbagai pihak, yaitu diantaranya:

1. Bagi Penulis

   Penelitian ini diharapkan dapat menambah dan meningkatkan pengetahuan dalam menganalisa jaringan menggunakan metode *malware* analisis dinamis dan metode *malware* analisis statis.
2. Bagi Mahasiswa

   Penelitian ini diharapkan dapat digunakan sebagai referensi dan sumber pengetahuan pada penelitian selanjutnya.
3. Bagi PT Nok Precision Component Batam

Penelitian ini diharapkan dapat membantu mengetahui kelemahan jaringan komputer dan langkah strategis menanggapi serangan *cybercrime* khususnya *malware* yang dapat mengganggu aktifitas perusahaan.