Abstrak

Ransomware adalah jenis perangkat lunak berbahaya yang mampu menonaktifkan fungsi komputer atau mengenkripsi semua file, yang mengakibatkan gangguan yang signifikan. Penelitian ini secara dinamis menganalisis perilaku ransomware pada sistem operasi Windows 11. Beberapa sampel ransomware dijalankan dan dianalisis untuk mendapatkan daftar perilaku ransomware yang digunakan dalam pengujian kinerja pada sampel-sampel tersebut. Topik ini penting karena serangan ransomware telah meningkat secara signifikan dan menjadi salah satu ancaman siber paling merusak. Serangan ransomware telah menyebabkan gangguan besar pada layanan seperti perbankan BSI, sehingga penting dalam era digital ini untuk memahami perilaku file atau proses yang mencurigakan dan bagaimana cara mengurangi ancaman tersebut.

Penelitian ini melakukan analisis dinamis terhadap perilaku ransomware pada sistem operasi Windows 11. Dalam lingkungan yang terisolasi menggunakan Mesin Virtual (VM), penelitian ini menggunakan alat seperti Process Monitor, Wireshark, dan ProcDOT untuk mengumpulkan data dan memvisualisasikan perilaku ransomware. Hasil dari penelitian ini mencakup kompilasi daftar perilaku ransomware yang digunakan untuk membangun sistem deteksi yang dapat mengidentifikasi sampel berdasarkan perilaku yang terdeteksi. Sistem deteksi yang dikembangkan menunjukkan tingkat deteksi yang baik, dengan persentase deteksi sebesar 69%. Hasil ini menunjukkan potensi signifikan dalam mengidentifikasi ancaman ransomware, meskipun masih ada ruang untuk perbaikan dan pengembangan lebih lanjut.

Kata kunci : perilaku, keamanan siber, sistem deteksi, analisis dinamis, ransomware