

ABSTRAK

Cryptocurrency seperti Monero semakin populer karena menawarkan privasi dan anonimitas yang tinggi. Namun, fitur ini juga menarik bagi pelaku kejahatan siber yang menggunakan teknik cryptojacking untuk menambang cryptocurrency tanpa sepengetahuan pengguna. Cryptojacking dapat menyebabkan kerusakan signifikan pada infrastruktur TI, termasuk penurunan kinerja sistem, konsumsi daya yang tinggi, dan potensi kerusakan perangkat keras. Laporan ini bertujuan untuk mengidentifikasi dan menganalisis pola lalu lintas jaringan yang terkait dengan aktivitas Monero menggunakan framework MITRE ATT&CK. Selain itu, laporan ini juga menyusun strategi mitigasi yang efektif untuk mengurangi risiko cryptojacking Monero. Hasil penelitian menunjukkan bahwa dengan memahami pola lalu lintas jaringan dan memanfaatkan MITRE ATT&CK Framework, organisasi dapat meningkatkan keamanan jaringan mereka dan melindungi sumber daya komputasi dari ancaman cryptojacking.

Kata Kunci: MITRE ATT&CK, Cryptocurrency, cryptojacking