BAB 1

PENDAHULUAN

1.1 Latar Belakang

Penggunaan mata uang kripto sebagai platform investasi telah meningkat pesat dalam beberapa waktu terakhir. Per 27 September 2020, terdapat 7.186 jenis mata uang kripto yang berbeda, dengan kapitalisasi pasar gabungan diperkirakan lebih dari 346 miliar USD. Dua mata uang kripto yang paling terkenal adalah Ethereum dan Bitcoin, dengan kapitalisasi pasar masing-masing sekitar 40 miliar dan 199 miliar USD. Pertumbuhan Ethereum dan Bitcoin telah memacu inovasi dalam teknologi blockchain dan keuangan terdesentralisasi (DeFi). Inovasi ini menciptakan peluang baru yang membuat keuangan menjadi efisien, transparan, dan inklusif, sehingga berpotensi mengubah cara kerja industri keuangan secara global [1].

Dengan meningkatnya aktivitas kripto, membuat perkembangan malware menjadi pesat. Salah satunya adalah *Cryptojacking*, merupakan serangan yang memanfaatkan sumber daya komputer korban dengan menargetkan kapasitas komputasi yang besar untuk penambangan mata uang digital demi keuntungan pribadi. Penelitian ini bertujuan untuk menyediakan metode pemantauan jaringan dengan mengintegrasikan metodelogi kerangka MITRE ATT&CK yang mampu mengidentifikasi aktivitas penambangan kripto ilegal [2]. Seperti Klien yang melakukan komunikasi melalui koneksi terenkripsi dengan server yang tersebar di seluruh Internet. Namun, dapat diidentifikasi dengan presisi dan akurat melalui pembelajaran mesin yang canggih.

MITRE ATT&CK merupakan kerangka kerja yang digunakan untuk mengklasifikasikan teknik, taktik, dan prosedur (TTP) yang digunakan oleh penyerang dalam serangan cyber. Dengan menganalisis pola log traffic, memudahkan untuk mengidentifikasi aktivitas mencurigakan yang menunjukkan adanya malware penambangan cryptocurrency [3].

Dengan menerapkan kerangka MITRE ATT&CK, studi ini diharapkan dapat meningkatkan pemahaman tentang cryptocurrency. Tetapi juga memberikan panduan praktis bagi pembaca guna meningkatkan kesadaran keamanan informasi demi menghadapi ancaman yang berkembang di lingkungan digital.

1.2 Rumusan Masalah dan Solusi

Dalam mendeteksi aktivitas awal penambangan kripto ilegal, korban sering menghadapi sejumlah tantangan, seperti penurunan performa sistem, peningkatan penggunaan sumber daya, kenaikan suhu perangkat, dan munculnya proses aplikasi yang tidak dikenal. Untuk mengatasi tantangan-tantangan ini, dapat diterapkan beberapa langkah seperti: Menggunakan alat pemantauan sistem untuk melacak CPU, GPU, dan Memori berupa Task Manager. Menganalisis trafik jaringan untuk menemukan pola komunikasi yang mencurigakan (anomali), yang bisa menunjukkan bahwa perangkat terhubung dengan server penambangan. Menggunakan perangkat lunak antivirus atau antimalware yang memiliki kemampuan untuk mendeteksi dan menghapus malware penambangan kripto. Menerapkan pemindaian keamanan yang dapat mengidentifikasi file atau proses yang tidak sah dan mencurigakan. Melakukan audit rutin terhadap konfigurasi perangkat dan aplikasi untuk mendeteksi adanya perangkat lunak yang tidak sah. Menerapkan kerangka MITRE ATT&CK terkait aktivitas penambangan ilegal. Dengan menerapkan langkah-langkah ini, diharapkan perangkat dapat terlindungi dari aktivitas berbahaya, termasuk penambangan kripto ilegal.

1.3 Tujuan

Tujuan yang diharapkan dengan adanya rumusan masalah dan solusi sebelumnya adalah sebagai berikut:

1. Menggunakan solusi keamanan yang kuat dan terintegrasi, termasuk antivirus, antimalware, dan perangkat lunak pemantauan sistem.
2. Mengadopsi teknologi deteksi berbasis kecerdasan buatan dan analitik untuk mengidentifikasi pola aktivitas yang tidak biasa (anomali) dengan mengintegrasikan kerangka MITRE ATT&CK.

3. Menjaga sistem dan perangkat lunak tetap diperbarui dengan patch dan pembaruan keamanan terbaru untuk mengurangi kerentanan yang bisa dimanfaatkan oleh penambang ilegal.
4. Melakukan audit sistem dan pemantauan secara rutin untuk mendeteksi dan mengatasi potensi ancaman sebelum menjadi masalah besar.

1.4 Batasan Masalah

Berikut ini beberapa batasan masalah yang akan menjadi tolak ukur dalam kajian ini:

1. Kajian ini akan berfokus pada analisis terkait aktivitas dari Cryptocurrency.
2. Ketergantungan pada data log sehingga analisis pola log traffic hanya efektif jika data log tersedia dan akurat. Ketersediaan data log yang tidak lengkap atau tidak akurat dapat membatasi kemampuan untuk mengidentifikasi aktivitas mencurigakan.
3. Kesulitan dalam membedakan aktivitas normal dan mencurigakan dikarenakan terdapat pola log traffic yang serupa.
4. Jika muncul malware baru yang lebih modern, Maka akan sulit untuk mendeteksi atau mencegahnya.
5. Biaya untuk implementasi dan pemeliharaan sistem dapat menimbulkan biaya yang signifikan bagi organisasi ataupun individu.

1.5 Penjadwalan Kerja Dan Timeline Penelitian

Selama melaksanakan kegiatan magang di Defenxor (PT. Defender Nusa Semesta), penulis mendapatkan jadwal masuk untuk melaksanakan magang dari hari Minggu - Rabu di setiap minggunya. Kemudian untuk jam masuk dibagi menjadi 3 bagian, yaitu: Shift Early, Middle, dan Late.

Berikut merupakan jadwal pekerjaan yang dilakukan guna menyelesaikan analisa terkait aktivitas dari Monero Crytocurrency.

Tabel 1. 1 Tabel penjadwalan kerja

No	Deskripsi Kerja	Maret				April				Mei				Juni				Juli				Agustus			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Diskusi																								
2	Analisa Awal																								
3	Identifikasi Kerentanan																								
4	Identifikasi Log																								
5	Penerapan Metodologi MITRE ATT&CK																								
6	Evaluasi																								
7	Penetapan Mitigasi & Risiko																								
8	Pengecekan Pada Host																								
9	Dokumentasi & Publikasi																								