ANALISIS DAN DETEKSI CRYPTOMINING STUDI KASUS VERUS

Nur Rosid Wakhid Wahyudi[1], Arief Ikhwan Wicaksono[2], Dedy Hariyadi[3]

INTISARI

Penambangan mata uang kripto telah menjadi fenomena global yang penting dalam beberapa tahun terakhir. Operasi ini memerlukan sumber daya komputasi yang signifikan untuk memvalidasi transaksi dan menambahkan blok baru ke blockchain. Namun, dalam beberapa kasus, penambangan mata uang kripto dilakukan secara ilegal atau tanpa izin, sering kali mengakibatkan penggunaan sumber daya jaringan tanpa izin. Untuk mendeteksi dan mencegah aktivitas penambangan mata uang kripto yang berbahaya, *port mirroring* adalah teknik yang memungkinkan administrator jaringan mengalihkan salinan lalu lintas jaringan dari satu atau lebih *port* ke *port* lain yang ditujukan khusus untuk pemantauan. Dengan menerapkan port mirroring pada perangkat jaringan, seperti *switch* atau *router*, analisis lalu lintas dapat dilakukan tanpa mengganggu operasi normal jaringan. Pencerminan port memungkinkan administrator untuk mencatat dan menganalisis semua jenis lalu lintas yang melalui jaringan. Ini termasuk lalu lintas yang dihasilkan oleh operasi penambangan mata uang kripto

Berdasarkan permasalahan tersebut, penelitian ini mengembangkan metode untuk mendeteksi aktivitas data mining. Metode yang digunakan disebut *port mirroring* menggunakan jaringan terbuka untuk memantau jaringan secara *real time*, menggandakan lalu lintas jaringan yang melewati aliran yang sama dengan mengelola *port mirroring* dengan mengidentifikasi serangan lalu lintas jaringan, kemacetan dan potensi lainnya. Selain mendiagnosis administrator, ancaman keamanan, dan mengidentifikasi lalu lintas dengan jalur perute-an yang menghubungkan perangkat pemantauan, lalu lintas data dapat dianalisis tanpa berdampak pada aliran awal yang sedang terjadi selama penambangan kripto. Pada penelitian ini dilakukan simulasi mining pada aplikasi *Verus Miner* 9000 yang berjalan pada jaringan *wifi* yang beroperasi pada segmen dengan sensor *Rasbery* yang mereplikasi data tanpa mengubah data asli, *p sek* dapat bekerja dengan baik tanpa adanya beban jaringan. Jaringan yang diamati langsung pada saat penambangan selama ini, masih relatif aman tanpa ada hambatan atau serangan yang dapat merugikan penambang diaplikasi *Verus*.

Berdasarkan penelitian yang dilakukan, kesimpulan dari penelitian ini adalah aplikasi *mailtrail* tidak mendeteksi serangan dari luar, maupun beban yang diterima pengguna saat menambang *cryptocurrency*, jaringan diklaim tidak terinfeksi oleh gangguan dari pihak lain. .

Kata kunci: *footprinting, activity scanning, repotting*

---

1 Mahasiswa Program Studi (S-1) Teknologi Informasi Universitas Jenderal Ahmad Yani Yogyakarta
2 Dosen Program Studi (S-1) Teknologi Informasi Universitas Jenderal Ahmad Yani Yogyakarta
3 Dosen Program Studi (S-1) Teknologi Informasi Universitas Jenderal Ahmad Yani Yogyakarta

ANALISIS DAN DETEKSI CRYPTOMINING STUDI KASUS VERUS

Nur Rosid Wakhid Wahyudi[1], Arief Ikhwan Wicaksono[2], Dedy Hariyadi[3]

ABSTRACT

Cryptocurrency mining has become an important global phenomenon in recent years. This operation requires significant computational resources to validate transactions and add new blocks to the blockchain. However, in some cases, cryptocurrency mining is carried out illegally or without permission, often resulting in unauthorized use of network resources. To detect and prevent malicious cryptocurrency mining activity, port mirroring is a technique that allows network administrators to redirect copies of network traffic from one or more ports to another port specifically designated for monitoring. By implementing port mirroring on network devices, such as switches or routers, traffic analysis can be performed without disrupting the normal operation of the network. Port mirroring allows administrators to log and analyze all types of traffic passing through the network. This includes traffic generated by cryptocurrency mining operations

Based on these problems, this study developed a method to detect data mining activity. The method used is called port mirroring using open networks to monitor the network in real time, doubling the network traffic passing through the same stream by managing port mirroring by identifying network traffic attacks, bottlenecks and other potential. Apart from diagnosing administrators, security threats, and identifying traffic by routing paths connecting monitoring devices, data traffic can be analyzed without impacting the initial flow that is occurring during crypto mining. In this research, a mining simulation was carried out on the Verus Miner 9000 application which runs on a wifi network that operates on segments with Rasbery sensors that replicate data without changing the original data, port mirroring can work properly without any network load. The network that has been observed directly during mining so far is still relatively safe without any obstacles or attacks that could harm miners in the Verus application.

Based on the research conducted, the conclusion of this study is that the mailtrail application does not detect external attacks, nor the load that users receive when mining cryptocurrency, the network is claimed not to be infected by interference from other parties.

.Keywords : footprint, performance analysis, problem solving

---

1 Mahasiswa Program Studi (S-1) Teknologi Informasi Universitas Jenderal Ahmad Yani Yogyakarta
2 Dosen Program Studi (S-1) Teknologi Informasi Universitas Jenderal Ahmad Yani Yogyakarta
3 Dosen Program Studi (S-1) Teknologi Informasi Universitas Jenderal Ahmad Yani Yogyakarta