*JTKSI (Jurnal Teknologi Komputer dan Sistem Informasi)*

JTKSI, Volume 6, Nomor 01, Januari 2023
E ISSN: 2620-3030; P ISSN: 2620-3022, pp.23-28
Accredited SINTA 4 Nomor 200/M/KPT/2020
http://ojs.stmikpringsewu.ac.id/index.php/jtksi

*Received: 30 Desember 2022; Revised: 4 Januari 2023; Accepted: 9 Januari 2023*

# Implementasi Cloudflare Zero Trust Dalam Mendeteksi Aktivitas Cryptojcking Pada Jaringan Komputer

**Sandi Adhar[1], Usep Saprudin[2]**
[1,2]Prodi Teknik Informatika, STMIK Dharma Wacana Metro, Metro, Lampung
[1,2]Jl. Kenanga No.3, Mulyojati, Kec. Metro Bar., Kota Metro, Lampung 34121
E-Mail: sandiadhar@gmail.com[1],usepsaprudin@gmail.com[2]

**Abstrak**

Dengan meningkatnya popularitas mata uang *crypto (cryptocurrency)* menyebabkan tingginya aktivitas penambangan *crypto*, penambangan *crypto* memerlukan sumber daya yang besar sehingga banyak *cyberciminal* melakukan aktivitas ilegal dengan mencuri akses ke komputer orang lain untuk digunakan menambang *cryptocurency (cryptojacking)*, hal ini dapat mengganggu kinerja dari sebuah komputer apabila komputer tersebut di gunakan dengan ilegal tanpa sepengetahuan pemilik komputer, selain itu *cryptominning* juga berjalan dengan memanfaatkan jaringan internet, *CPU usage* dan sumber listrik dari komputer korban, untuk itu pada penelitian ini akan melakukan implementasi layanan *software as service (Saas)* dari cloudflare zero trust yang dapat mendeteksi dan mengantisipasi aktifitas *cryptojacking* pada jaringan internet guna melakukan antisipasi serangan, clouflare zero trust akan di pasang pada jaringan menggunakan perantara routerboard MikroTik, selain itu penulis akan melakukan uji coba serangan (penetrasi *testing*) dengan melakukan aktifitas *crypto mining* pada komputer di dalam sebuah jaringan dan melakukan analisa apakah cloudflare zero trust mampu mendeteksi dan mengantisipasi serangan tersebut.

**Kata Kunci:** *Cryptojacking*, Deteksi *Malware*, *signature-based*, jaringan, *firewall*

***Abstract***

*With the increasing popularity of cryptocurrency (cryptocurrency) causing high crypto mining activity, crypto mining requires large resources so that many cybercriminals carry out illegal activities by stealing access to other people's computers to be used to mine cryptocurrencies (cryptojacking), this can interfere with the performance of a computer if the computer is used illegally without the knowledge of the computer owner, apart from that crypto mining also runs by utilizing the internet network, CPU usage and the power source from the victim's computer, for this reason this research will implement software as service (Saas) services from Cloudflare zero trust that can detect and anticipate cryptojacking activities on the internet network in order to anticipate attacks, Cloudflare zero trust will be installed on the network using the MikroTik routerboard intermediary, besides that the author will conduct an attack trial (penetrator si testing) by carrying out crypto mining activities on computers in a network and analyzing whether Cloudflare Zero Trust is able to detect and anticipate these attacks.*

***Keywords:*** *Cryptojacking, Malware detection, signature-based, networking, firewall*

## I. PENDAHULUAN

Pada tahun 2009 bitcoin menjadi cryptocurency pertama yang hadir dan diperkenalkan ke dunia[1], cryptocurrency sendiri adalah mata uang digital yang terenkripsi dan setiap transaksinya di catat secara desentralisasi[2], untuk mendapatkanya orang harus melakukan penambangan[3], namun karena device yang digunakan untuk menambang cukup mahal maka meningkatkan aktifitas cybercriminal untuk mengambil akses komputer orang lain guna melakukan.mining (cryptojacking)[4], hal ini senada dengan data yang di ungkapkan.oleh ENISA cryptojacking menjadi serangan yang cukup banyak dilakukan dan mencapai rekor tertinggi pada tahun 2021[5], hal ini tentu harus di waspadai dan di antisipasi.

Beberapa literatur yang berhubungan dengan aktivitas cryptojacking diantaranya yaitu Meland pada tahun 2019 menjelaskan bahwa cryptojacking berbeda dengan serangan lainya yang melakukan aktifitas pencurian data dan inteuprsi data, cryptojacking lebih memilih sembunyi dan terus mengkonsumsi resource yaitu bandwith dan CPU pengguna untuk terus melakukan crypto mining, terdapat dua type dalam melakukan cryptojacking yaitu mendistribusikannya melalui malware yang berfungsi untuk melakukan mining sedangkan tipe serangan cryptojacking yang ke dua adalah menaruh sebuah javascript pada website

publik sehingga apabila website di kunjungi oleh pengguna, pengguna akan mengeksekusi javascript yang ada pada website yang berfungsi untuk melakukan mining[6].

Beberapa cara dapat dilakukan dalam mendeteksi aktifitas cryptojacking, Hong pada tahun 2018 melakukan perayapan pada 100.000 website teratas guna mencari halaman dari setiap situs tersebut dan mencari kemungkinan website telah di jangkiti script mining berbasis website dan memperkirakan bahwa cryptojacking yang menjangkiti website tersebut dapat menjadi ancaman bagi 10 juta pengguna web dan daya listrik sebanyak 278.000 kWh setiap hari atau setara dengan konsumsi energy bagi kota dengan populasi 9300 orang [7]. Selain menjangkiti website beberapa cybercriminal membajak perangkat jaringan guna melakukan DNS redirection, sehingga pengguna di paksa mengakses website yang terjangkiti script cryptojacking [8]. Beberapa langkah dalam menanggulangi cryptojacking di antaranya adalah menonaktifkan layanan yang tidak digunakan, melengkapi keamanan komputer menggunakan antivirus dan tidak menggunakan software bajakan [9].

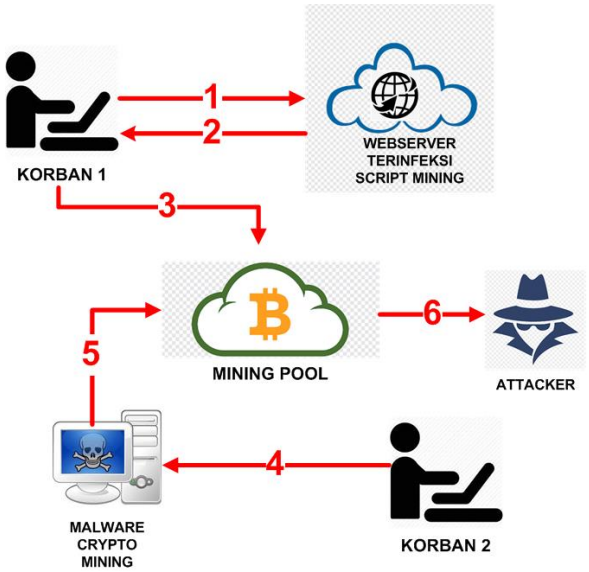
Dari beberapa literatur yang telah di sampaikan beberapa melakukan cara antisipasi dari sisi pengguna, dengan menggunakan antivirus yang tentunya bagi administrator jaringan akan sangat sulit untuk mengatur pengguna yang banyak, selain itu beberapa metode yang dilakukan dalam mendeteksi cukup sulit untuk dilakukan, dari masalah cryptocurrency yang sangat mengancam dan keterbatasan sumberdaya yang dimiliki tentunya akan sangat menghambat bagi sebuah instansi yang belum memiliki sumber daya yang memadai, untuk itu penulis mencoba menggunakan jasa dari cloud yang mampu membantu instansi kecil dalam menyediakan software as service yang terjangkau [10]. Penelitian ini akan memanfaatkan clouflare zero trust yaitu salah satu layanan software as service yang mampu mendeteksi dan mengantisipasi serangan cryptojacking, penulis akan melakukan uji coba serangan dengan menginstal aplikasi crypto mining pada web browser dan melakukan analisis apakah clouflare zero trust mampu mendeteksi dan mengantisipasi serangan tersebut.

## II. TINJAUAN PUSTAKA

### A. *Cryptojacking*

Cryptojacking merupakan sebuah aktifitas illegal dalam menggunakan resource pengguna, baik itu CPU, internet maupun sumber daya listrik guna melakukan aktifitas penambangan cryptocurrency [11].

Menurut Zimba et.al, menjelaskan bahwa terdapat beberapa cara dalam melakukan aktifitas cryptojacking, seperti yang ditunjukan pada gambar 1 dibawah ini.




**Gambar 1**. Anatomi cryptomining menurut zimba

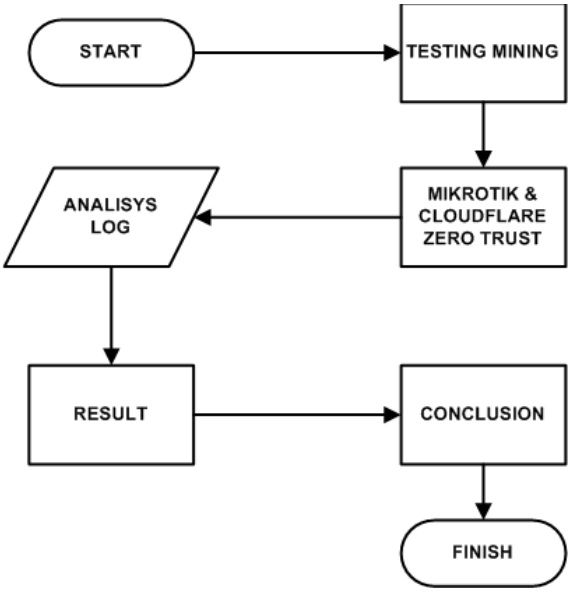
Serangan type pertama yaitu pengguna mengakses sebuah situs yang terinfeksi script cryptojacking, ketika pengguna mentriger script tersebut maka secara tidak sadar computer pengguna telah melakukan aktifitas mining, sedangkan pada type serangan ke dua computer korban yang telah terinfeksi malware cryptojacking akan melakukan aktifitas mining tanpa kesadaranya [12].

### B. *Cloudflare Zero Trust*

Cloudflare zero trust merupakan sebuah layanan yang di berikan oleh cloudflare, salah satu produk dari cloudflare zero trust yaitu cloudflare gateway berfungsi untuk menjaga keamanan cyber yang dapat mencegah malware, ransomware, phising, command&control, shadow IT dan resiko keamanan internet lainya [13]. Cloudflare menyediakan layanan Software as a service (SaaS). Layanan SaaS tidak membutuhkan biaya yang besar, baik dalam kebutuhan hardware, listrik bahkan personil yang melakukan maintenance, sehingga akan mudah di implementasikan pada perusahaan yang masih berkembang [14].

## III. METODE PENELITIAN

Pada penelitian ini tahap yang dilakukan adalah melakukan uji coba serangan pada jaringan yang telah di lindungi oleh *Cloudflare*. Berikut ini gambar 2 akan menunjukan proses penelitian yang dilakukan.




**Gambar 2**. Alur Penelitian

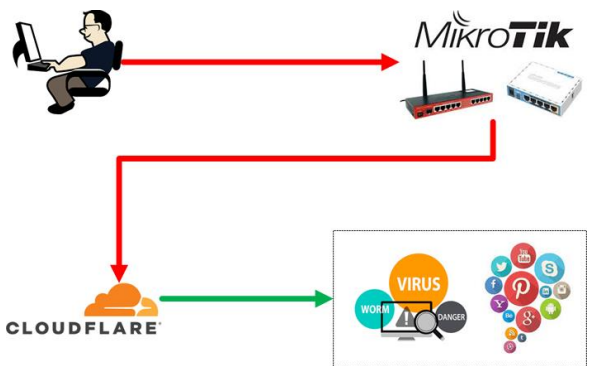
Merujuk pada penelitian [15], yang melakukan uji coba serangan pada sistem yang telah di lindungi. Hal ini menginspirasi untuk melakukan analisis dari log cloudflare gateway dan melihat apakah cloudflare gateway mampu mendeteksi serangan dari aktifitas crypto mining, apabila berhasil maka sistem yang dibangun akan mampu mendeteksi aktifitas cryptojacking.

*A. Proses Perancangan*

Proses perancangan yang dilakukan adalah dengan menggunakan metode DIO Life cycle, DIO sendiri merupakan sebuah akronim dari Design, Implementation dan Operate [16], pada tahap design akan dilakukan sebuah pemetaan apa saja yang akan dilakukan dalam implementasi Cloudflare Gateway dalam mendeteksi cryptojacking, setelah itu langkah yang dilakukan dengan melakukan implementasi dan mengoperasikan mekanisme yang sudah dibuat.

*B. Analisis Kinerja Cloudflare Gateway*

Mekanisme yang telah di bangun yaitu proses implementasi cloudlflare zero trust dengan memanfaatkan layanan cloudflare gateway akan di pasang pada router mikrotik, sehingga trafik dari pengguna akan di teruskan oleh mikrotik ke cloudlfare gateway. Berikut ini gambar 3 yang menunjukan proses kerja cloudflare gateway.




**Gambar 3**. Analisis kinerja cloudflare gateway

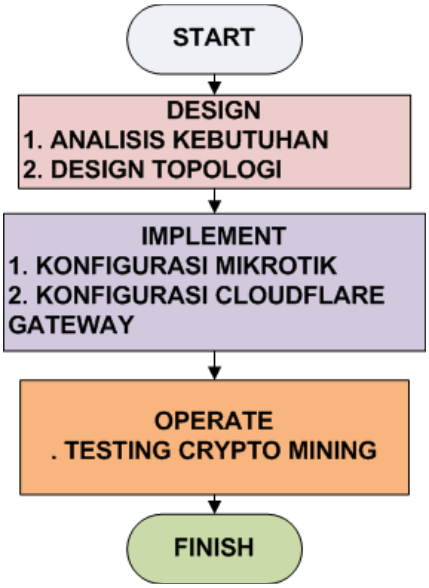
Proses pada gambar 3 menunjukan PROSES testing di jalankan dengan melakukan mining menggunakan jaringan yang di lindungi cloudflare gateway lalu akan di lakukan analisis dari log yang ada pada dashboard cloudflare zero trust apakah dapat mengenali serangan tersebut.

## IV. HASIL DAN PEMBAHASAN

Proses penelitian implementasi cloudflare zero trust dalam mendeteksi aktivitas cryptojcking pada jaringan komputer, memiliki beberapa tahapan.

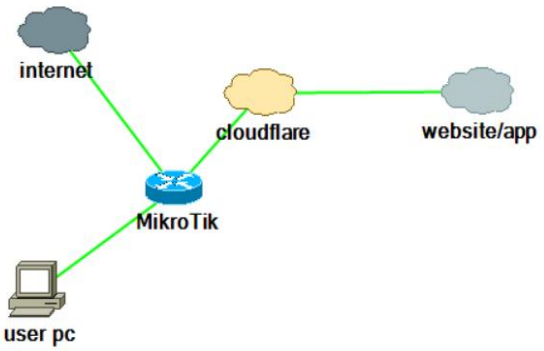
*A. Perancangan*

Tahapan dalam implementasi akan menggunakan metode DIO Lifecycle yang akan dijelaskan pada gambar 4 di bawah ini.




**Gambar 4**. Alur Implementasi cloudflare gateway

Pada tahap desain peneliti membutuhkan beberapa peralatan (kebutuhan) sebelum melakukan implementasi, kebutuhan berupa hardware yaitu routerboard MikroTik, pada penelitian ini routerboard Mikrotik yang di gunakan adalah CCR1072-1G-8S+ MikroTik akan digunakan untuk memasang Cloudflare gateway. Berikut ini merupakan gambar 5 yang merupakan topologi yang akan di bangun untuk implementasi cloudflare zero trust.

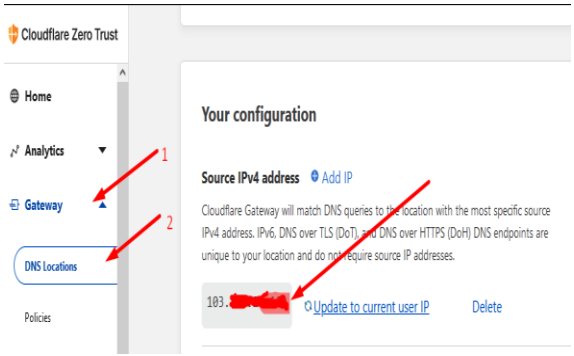



**Gambar 5**. Topologi cloudflare gateway

Dari topologi pada gambar 5, maka *user* akan menggunakan *DNS* (domain name server) dari cloudflare gateway, sehingga setiap *host* yang di kunjungi pengguna akan melalui cloudflare gateway dan cloudflare akan memfilter domain yang dicurigai sebagai aktifitas *cryptojacking*.

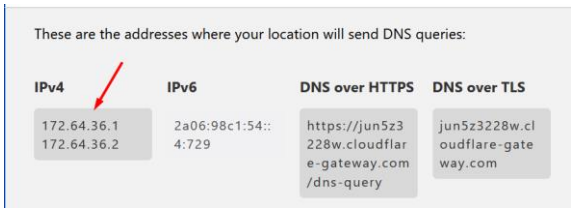
## B. *Implementasi*

Pada tahap implementasi akan di lakukan dengan mengkonfigurasi Mikrotik dan cloudflare gateway, berikut ini beberapa langkah yang di lakukan untuk mengkonfigurasi MikroTik dan cloudflare gateway. Tahap awal yang dilakukan dalam melakukan implementasi cloudflare zero trust adalah dengan menambahkan internet protocol (IP) address dari jaringan ke dashboard yang ada pada cloudflare zero trust, seperti pada gambar 6 di bawah ini.



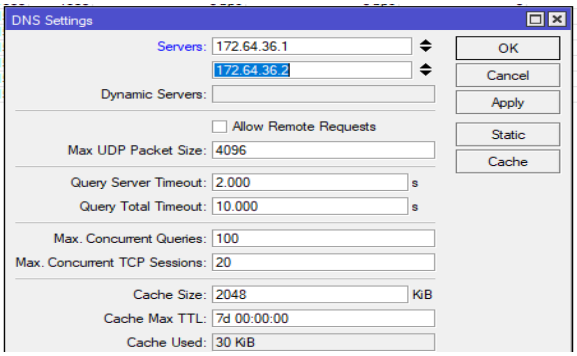

**Gambar 6**. Add IP address pada cloudflare

Proses yang ditunjukan pada gambar 6 merupakan proses pencocokan cloudflare apakah identitas jaringan cocok dengan DNS yang akan di pasang pada MikroTik, dapat dikatakan ini adalah proses autentikasi sebuah hardware yang terkoneksi dengan layanan telah sesuai dengan DNS yang akan di berikan oleh cloudflare gateway. Setelah menambahkan IP Address jaringan, maka cloudflare gateway akan memberikan DNS yang akan di pasang pada MikroTik, Berikut ini merupakan gambar 7 menunjukan DNS yang akan kita pasang pada MikroTik.




**Gambar 7**. DNS yang akan digunakan MikroTik

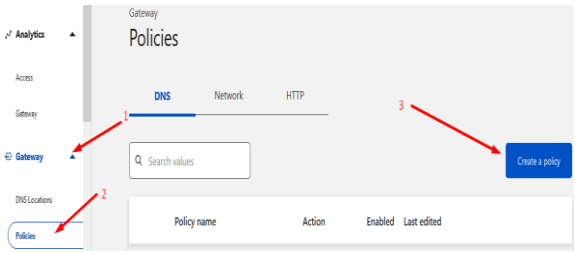
Setelah mendapatkan DNS yang di berikan cloudflare gateway maka selanjutnya adalah proses konfigurasi pada router MikroTik, yaitu dengan melakukan konfigurasi pada DNS Mikrotik. Berikut ini gambar 8 yang menunjukan proses penambahan DNS cloudflare ke MikroTik.




**Gambar 8**. *ADD DNS* cloudflare pada MikroTik

Setelah konfigurasi DNS pada MikroTik maka trafik dari pengguna akan di teruskan ke cloudflare sebelum menuju sebuah website atau aplikasi yang menggunakan jaringan internet.

Selanjutnya setelah DNS terpasang pada MikroTik proses selanjutnya adalah membuat policy (kebijakan) atau aturan rule pada dashboard cloudflare zero trust untuk mendeteksi aktifitas cryptojacking, berikut ini gambar 9 yang menunjukan proses pembuatan rule untuk mendeteksi aktifitas cryptojacking.




**Gambar 9**. Membuat rule pada cloudflare

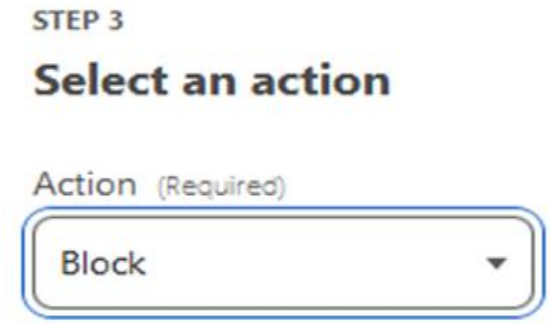
Setelah memilih menu create policy maka hal yang di lakukan selanjutnya adalah mengisi form, pada step pertama kita akan mengisi policy name dengan nama rule yang akan kita buat serta deskripsinya, seperti yang ditunjukan oleh gambar 10 di bawah ini.


**Gambar 10**. Mengisi policy name

Tahap selanjutnya kita akan mengisi ekspresi yang akan di *filter*, form ini terdiri dari beberapa isian yang akan menjadi rule cloudflare gateway berikut ini gambar 11 yang menunjukan pengisian form ekspresi yang akan di isi.

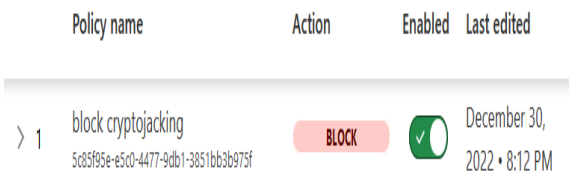

**Gambar 11**. Mengisi form ekspresi

Pada gambar 11, kolom selector adalah kategori yang akan kita filter yaitu "security category", selanjutnya pada kolom operator di isi dengan "in" dan pada kolom value di isi dengan "Cryptomining" Artinya rule yang dibuat akan mendeteksi aktifitas cryptomining yang ada pada jaringan. Step terakhir adalah mengisi form action seperti pada gambar 12 di bawah ini.




**Gambar 12**. Mengisi form action

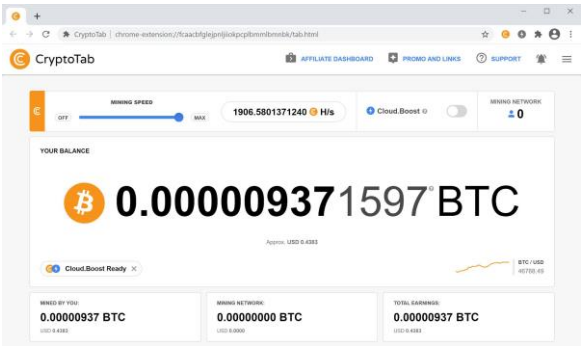
Setelah mengisi form pembuatan rule maka selanjutnya adalah proses menyimpan dengan menekan tombol simpan yang ada pada form, setelah tersimpan maka rule / policy akan di tampilkan pada dashboard seperti pada gambar 13 di bawah ini.




**Gambar 13**. Rule / policy yang dibuat.

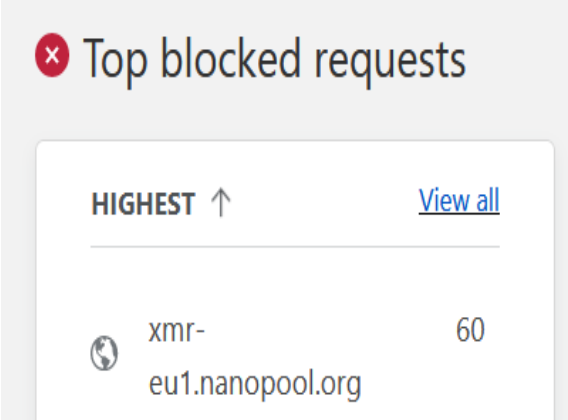
*C. Tahap Operate dan uji coba*

Setelah proses konfigurasi yang di lakukan selesai maka selanjutnya adalah proses testing, proses ini akan membuktikan apakah cloudflare zero trust dengan layanan cloudflare gateway dapat mendeteksi aktifitas mining yang di lakukan oleh browser. Tahap yang dilakukan adalah dengan melakukan instalasi aplikasi browser mining crypto pada sebuah computer, setelah menginstal aplikasi tersebut selanjutnya adalah menjalankan aplikasi browser mining tersebut, seperti di tunjukan pada gambar 14 dibawah ini.




**Gambar 14**. Menjalankan cryptomining via browser

Untuk mengetahui apakah cloudflare zero trust mendetekai aktifitas mining tersebut, hal yang dilakukan adalah melakukan checking pada dashboard cloudflare zero trust pada menu analytics, dan pilih menu gateway sehingga muncul halaman seperti pada gambar 15 di bawah ini.




**Gambar 15**. Cloudflare mampu mendeteksi aktifitas mining

Pada gambar 15 menunjukan bahwa cloudflare melakukan blocking pada domain yang menuju xmr-eu1.nanopool.org yang merupakan domain pool mining cryptocurrency, sehingga dapat di simpulkan bahwa mekanisme yang di bangun berhasil mendeteksi aktifitas mining yang di lakukan.

*D. Analisis Hasil penelitian*

Dari hasil uji coba yang dilakukan mekanisme deteksi cryptojacking dengan memanfaatkan layanan *cloud Saas (software as service)* menggunakan cloudflare zero trust dengan *service* cloudflare gateway dapat mendeteksi serangan *cryptojacking* yang apa pada jaringan komputer. Cloudflare zero trust dapat di pasang pada jaringan dengan memanfaatkan routerboard mikrotik, di mana pengguna jaringan akan menggunakan DNS cloudflare gateway yang terpasang pada routerboard MikroTik, dengan demikian pengguna jaringan akan di analisis oleh mesin yang ada pada cloudflare zero trust, sehingga apabila terdapat *host* yang akan di kunjungi pengguna dan mengandung unsur *crypto mining* akan di blokir oleh cloudflare gateway, hal ini tentunya lebih efisien tanpa harus menyiapkan *resource* yang besar serta tidak membutuhkan konfigurasi yang sulit pada *firewall*

MikroTik, selain itu biaya yang di butuhkan juga sangat terjangkau.

Hasil pada gambar 15 menunjukan *URL (Uniform resource locator)* atau domain yang beralamat pada xmr-eu1.nanopool.org yang merupakan situs mining yang di gunakan dalam proses uji coba penetrasi *testing* telah berhasil di blokir sebanyak 60 kali, dari hal tersebut maka di simpulkan bahwa penelitian telah berhasil dalam memanfaatkan cloudflare zero trust di dalam mendeteksi dan mengantisipasi serangan *cryptojacking* yang ada pada jaringan komputer, sehingga jaringan terlindungi dari serangan *missuse* (serangan yang menargetkan jaringan atau komputer yang tidak semestinya).

## V. KESIMPULAN

Dari hasil testing yang dilakukan, cloudflare zero trust dengan fitur cloudflare gateway, mampu mendeteksi aktifitas mining yang di lakukan, maka dapat di katakan bahwa cloudflare zero trust mampu mendeteksi dan mengantisipasi serangan cryptojacking, proses konfigurasi yang mudah dan dengan biaya minimal, sehingga cara ini dapat di implementasi oleh instansi atau perusahaan kecil. Dari proses penelitian ini yang memanfaatkan cloudflare zero trust dengan fitur cloudflare gateway dapat mendeteksi cryptojacking pada jaringan, untuk itu saran berikutnya adalah dapat mengimplementasikan cloudflare zero trust dalam mendeteksi dan mengantisipasi serangan lain, seperti malware, ransomware, worm, virus dan lainya.

## DAFTAR PUSTAKA


[1] F. Gomes and M. Correia, "Cryptojacking Detection with CPU Usage Metrics," IEEE Xplore, Nov. 01, 2020. https://ieeexplore.ieee.org/document/9306696 (accessed Dec. 30, 2022).

[2] I. Petrov, L. Invernizzi, and E. Bursztein, "CoinPolice:Detecting Hidden Cryptojacking Attacks with Neural Networks," arxiv.org, Jun. 2020, [Online]. Available: https://arxiv.org/abs/2006.10861

[3] D. Tanana and G. Tanana, "Advanced Behavior-Based Technique for Cryptojacking Malware Detection," IEEE Xplore, Dec. 01, 2020. https://ieeexplore.ieee.org/abstract/document/9310048 (accessed Jan. 01, 2022).

[4] Tanana, "Behavior-Based Detection of Cryptojacking Malware," IEEE Xplore, May 01, 2020. https://ieeexplore.ieee.org/abstract/document/9117732

[5] Lella, Marianthi Theocharidou, E. Tsekmezoglou, and Apostolos Malatras, ENISA Threat Landscape 2021. 2021.

[6] P. H. Meland, B. H. Johansen, and G. Sindre, "An Experimental Analysis of Cryptojacking Attacks," Secure IT Systems, pp. 155–170, 2019, doi: 10.1007/978-3-030-35055-0_10.

[7] G. Hong et al., "How You Get Shot in the Back," Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Jan. 2018, doi: 10.1145/3243734.3243840.

[8] J. M. Ceron, C. Scholten, A. Pras, E. Lastdrager, and J. Santanna, "Characterising attacks targeting low-cost routers: a MikroTik case study (Extended)," arXiv:2011.01685 [cs], Nov. 2020, Accessed: Dec. 30, 2022. [Online]. Available: https://arxiv.org/abs/2011.01685

[9] "Laporan Tahunan Monitoring Keamanan Siber Tahun 2021 | bssn.go.id." https://bssn.go.id/laporan-tahunan-monitoring-keamanan-siber-tahun-2021/ (accessed Dec. 30, 2022).

[10] I. P. Saputra, R. Yusuf, and U. Saprudin, "IMPLEMENTASI CLOUD COMPUTING SEBAGAI RADIUS SERVER PADA JARINGAN INTERNET ROUTER MIKROTIK," Journal Computer Science and Informatic Systems : J-Cosys, vol. 1, no. 2, Jul. 2021, doi: 10.53514/jc.v1i2.67.

[11] C. Hayes, "The Evolution of Cryptojacking - ProQuest," www.proquest.com, 2021. https://www.proquest.com/openview/fa6c725b1d6b730a30eaf2670ebb7e6e/1?pq-origsite=gscholar&cbl=18750&diss=y

[12] A. Zimba, Z. Wang, M. Mulenga, and N. H. Odongo, "Crypto Mining Attacks in Information Systems: An Emerging Threat to Cyber Security," Journal of Computer Information Systems, pp. 1–12, May 2018, doi: 10.1080/08874417.2018.1477076.

[13] "Secure Web Gateway | Threat Protection," Cloudflare. https://www.cloudflare.com/products/zero-trust/gateway/

[14] A. Öberg, "WHAT IS ZERO TRUST - and How Can It Be Implemented?," Dec. 2022, Accessed: Dec. 30, 2022. [Online]. Available: https://www.theseus.fi/bitstream/handle/10024/788457/Oberg_Andre.pdf?sequence=2

[15] I. P. Saputra, E. Utami, and A. H. Muhammad, "Comparison of Anomaly Based and Signature Based Methods in Detection of Scanning Vulnerability," IEEE Xplore, Oct. 01, 2022. https://ieeexplore.ieee.org/abstract/document/9946485 (accessed Dec. 30, 2022).

[16] A. Hidayat, I. P. Saputra, and A. Bowo, "Bot Monitoring Jaringan Pada BMT Mentari Lampung Timur Menggunakan Mikrotik Dan API Telegram," JTKSI (Jurnal Teknologi Komputer dan Sistem Informasi), vol. 5, no. 3, Sep. 2022, doi: 10.56327/jtksi.v5i3.1291.