MEMBANGUN SISTEM PENDETEKSI MALWARE CRYPTOMINING

"(Building System Detector Malware Cryptomining)"

[1]Rifqi Rulliyansyah, [2]Setia Juli Irzal Ismail, S.T., M.T. [3] Lisda Meisaroh, S.Si., M.Si.
[1,2,3]Fakultas Ilmu Terapan Telkom University, Bandung
[1]rifqirulliyansyah@studemt.telkomuniversity.ac.di [2]jul@tass.telkomuniversity.ac.id
[3]lisdameisaroh@telkomuniversity.ac.id

ABSTRAK

Sistem membuat rancangan keamanan pada jaringan internet dan semua jenis file yang dapat menjadi indikasi malware namun semakin berkembang nya kemajuan security system pada jaringan dan internet maka setiap virus pun semakin mematenkan fungsi dan kerugian pada setiap pengguna yang terkena pada virus tersebut.Cryptomining merupakan serangan malware yang dapat menggunakan system operasi dan seluruh resource-nya pada sebuah PC untuk melakukan data mining untuk mendapatkan file Crypto currency/E-money pengguna Cryptomining sendiri dan web site yang terkena efek malware injeksi tersebut mendapatkan kerugian data mining.

Kata Kunci:Security network,malware,Cryptomining

ABSTRACT

The system makes security plans on the internet network and all types of files that can be indications of malware, but the more advances in security systems on the network and the internet are developing, so each virus is increasingly patenting functions and losses to each user who is affected by the virus. Cryptomining is a malware attack that can use the operating system and all of its resources on a PC to perform data mining to get Crypto currency / E-money files for Cryptomining users themselves and web sites affected by the injection malware get data mining losses.

Keywords: Security network,malware,Cryptomining.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Cryptomining merupakan sebuah malfungsi yang dapat merugikan banyak pengguna PC ataupun laptop.Cryptomining merupakan serangan malware yang dapat menggunakan system operasi dan seluruh resource-nya pada sebuah PC untuk melakukan data mining untuk mendapatkan file Crypto currency/E-money . contoh pada kasus yang terjadi pada situs web makanan cepat saji di Indonesia yaitu bkdelivery.co.id secara tidak langsung web site tersebut mendapatkan injeksi malware data untuk menguntungkan para pengguna Cryptomining sendiri dan web site yang terkena efek malware injeksi tersebut mendapatkan kerugian data mining di mana situs makanan cepat saji tersebut akan teralihkan ke situs mining coin.co dari hal ini semua data web site akan terpakai untuk data mining, denga adanya kasus seperti hal yang di ceritakan maka dari itu akan dibangun system pendeteksi Cryptomining yang akan mendeteksi malware dengan menggunakan tools dari CryptoStalker.

1.2 Tujuan

Adapun tujuan dari proyek akhir ini adalah :

1. Membangun system pendeteksi cryptomining
2. Dengan mendeteksi ada nya file injeksi malware yang akan menjadi data mining

1.3 Definisi Operasional

Adapun definisi operasional yang ada dalam laporan proyek akhir ini adalah sebagai berikut:

1. CryptoStalker. Merupakan sebuah tools yang akan mendeteksi file currency yang rusak atau terdeteksi virus malware

2. CryptoMining sebagai perantara pendeteksi ada nya crypto file yang terdeteksi malware atau tidak nya

3. Bracket atau Go-lang Merupakan basis script file yang akan menjadi source code dalam crypto file

1.4 Rumusan Masalah

Bedasarkan latar belakang yang telah diuraikan diatas, maka permasalahan yang dibahas adalah :

1. Bagaimana cara mendeteksi Malware Cryptomining?

2. Bagaimana melakukan Pengujian Sistem deteksi pada Malware Cryptomining?

1.5 Batasan Masalah

Batasan masalah yang ada adalah sebagai berikut :
1. Aplikasi pendeteksi malware yang kurang akurat.
2. Pengujian Hanya dilakukan pada system operasi windows
3. Perangkat keras yang di mencapai untuk melakukan mining
4.Memerlukan bentuk data mining dalam pengujian system

1.6 Metode Pengerjaan

Metodologi yang dilakukan dalam penulisan dan penyusunan Proyek Akhir ini adalah sebagai berikut

1. Studi Literatur Proses pencarian informasi dan referensi yang berkaitan dengan proyek akhir.

2. Analisis dan Perancangan
Analisis dilakukan mulai dari hardware sampai dengan software yang dibutuhkan dalam membangun prototype yang akan mengacu pada perancangan program yang telah dibuat berdasarkan data yang sudah ada.

3. Pengujian Prototype atau Aplikasi
Pengujian Prototype dilakukan dengan mencoba program yang telah dibuat dengan melakukan pengukuran kadar gula darah normal dan tidak normal untuk mengetahui berhasil atau tidaknya prototype tersebut.

4. Penyusunan Laporan Langkah terakhir ini semua metode, konfigurasi, dan dokumentasi yang telah terkumpul dibuat menjadi laporan proyek akhir.

BAB II TINJAUAN PUSTAKA

2.1 Penelitian sebelumnya

Penanganan Cryptojacking Menggunakan Pattern Matching Analysis Penulis Arief Dwi Yulianto
Penelitian ini membuat perancangan model in-browser-mitigation menggunakan ekstensi pada Google Chrome terhadap cryptojacking dengan metode Taint Analysis. Cryptojacking (juga disebut malicious cryptomining) adalah threat model baru menggunakan resource CPU secara sembunyi untuk ”mining” suatu cryptocurrency pada browser. Dampaknya berupa kenaikan CPU Usage dan performa sistem yang lambat. Metode yang digunakan pada penelitian ini adalah pemodelan serangan dengan abuse case menggunakan teknik penyerangan Man-In-The-Middle (MITM) sebagai acuan untuk mitigasi. Perancangan model yang diusulkan dapat memberikan notifikasi kepada pengguna browser jika serangan cryptojacking terjadi.Maka dari itu pengguna dapat mengetahui karakteristik skrip yang berjalan pada background website. Hasil dari penelitian ini dapat memitigasi serangan cryptojacking, dari 100 sampel random website, model yang diajukan dapat mendeteksi 19 website yang terindikasi menginjeksi cryptojacking..

2.2 Teori

2.2.1 Malware

Adalah sebuah virus atau perangkat lunak yang di rancang pada system computer yang mampu merusak atau menghentikan seluruh program yang sedang berjalan dan dapat menyebabkan beberapa file ataupun system operasi malware dapat memasuki system computer kita melalui internet,mendownload sebuah file , atau pengiriman email.

2.2.2 CryptoMining

Cryptomining adalah serangan Cyber yang dapat merugikan para user dalam hal mining bitcoin atau uang elektronik yang biasa memining dari satu user ke user lain dengan mengandalkan resource dari beberapa user Pc atau laptop untuk mendapatkan sebuah file CryptoCurrency.

2.2.3 Currencyfile atau Cryptocurrency

Secara etimologis,cryptocurrency tersusun dari dua kata, yaitu Crypto yang berarti Cryptography atau Bahasa persandian dalam dunia computer sedangkan currency ialah mata uang jadi dapat di definisikan bahwa Crptocurrency adalah sebuah mekanisme mata uang digital yang dapat di gunakan secara virtual melalui jaringan internet yang di lindungi dengan sebuah sandi kompuer yang rumit.

2.2.4 CryptoStalker berbasis Go-lang atau Brcaket

Tool detector yang merupakan basis source code dari bin bash atau Go-lang yang mampu mendeteksi ada nya file yang terdeteksi malware atau file yang sudah korup setiap file akan di scan dengan CryptoStalker yang di mana akan memudahkan user untuk mengesekusi file tersebut.

BAB III ANALISIS PERANCANGAN

3.1 Analisis

3.1.1 Gambaran Sistem Saat Ini (atau Produk)

Adapun gambaran sistem saat ini dalam pembahasan proyek akhir ini, sebagai berikut : Gambar 3.1 Merupakan Blok diagram sistem saat ini, adalah sistem penyerangan pada website ataupun file namun pada saat ini .

Dengan cara

-Penyerang melakukan scanning Ip untuk mendapat akses ke Ip target

-komputer target akan di injeksikan malware data mining

-malware akan melakukan mining Cryptocurrency

-lalu Malware tersebut akan mengirim E-money ke wallet penyerang.

3.2 Perancangan

3.2.1 Gambaran Sistem Usulan

gambaran sistem usulan, pengecekan file/Script dengan cara menganalisa terlebih dahulu, lalu program akan mendeteksi adanya data mining atau tidak, jika terdapat injeksi malware maka user akan mendapat notifikasi oleh program bahwa ada data mining pada file/Script tersebut .

Dari blok diagram di atas, sistem yang akan diusulkan dapat dibagi ke dalam 3 bagian, yaitu:

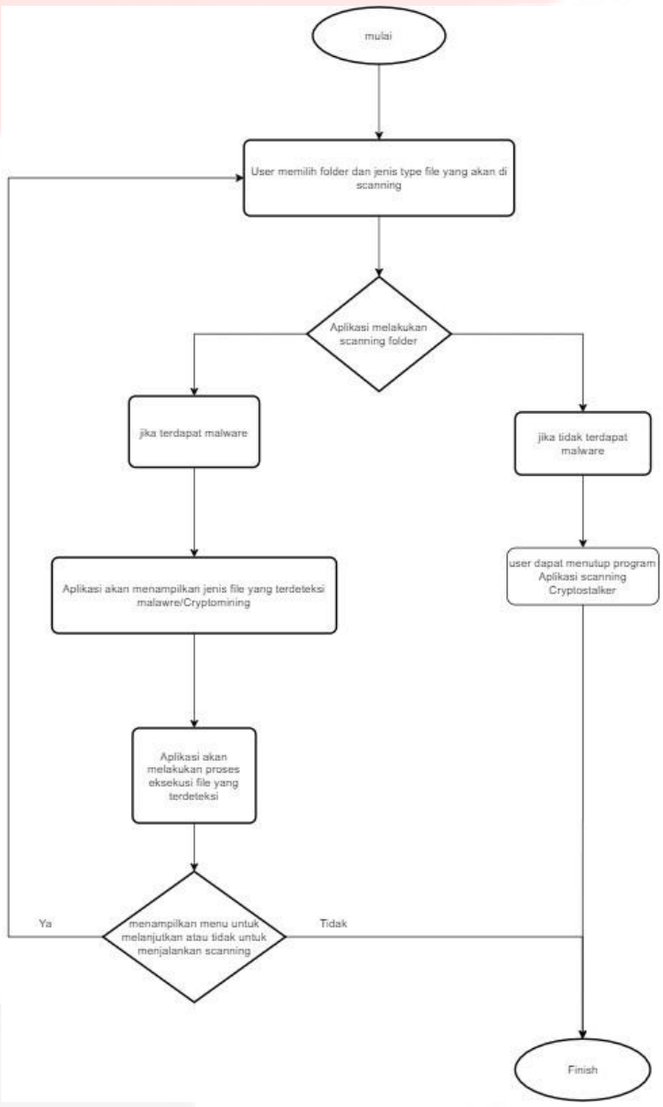
a. INPUT, yaitu bagian yang berfungsi sebagai pendeteksi ada nya malware Cryptomining.

b. PROSES, yaitu bagian yang berfungsi untuk menghentikan file yang terdeteksi malware Cryptomining.

OUTPUT, yaitu bagian yang berfungsi untuk menampilkan hasil deteksi malware Cryptomining dan memberikan user notifikasi kepada user..

3.2.2 Flowchart Sistem Usulan

Sistem Usulan ini dibagi ke dalam 3 bagian, yaitu input, proses, dan output. Gambar 3.3 merupakan flowchart sistem usulan.



Gambar 3. 2.2 Flowchart system usulan

3.2.3 Cara Kerja

Berikut ini adalah cara kerja sistem yang dibuat dalam proyek akhir ini:

1. Mengaktifkan Go-lang yang akan mendeteksi file.

2. Kemudian menginput file yang akan di scanning

3. Aplikasi akan melakukan scanning folder.

4. Jika tidak terdapat file yang terinfeksi malware maka user dapat menutup apilkasi.

5. Jika terdapat malware maka file tersebut akan di tampilkan kedalam jenis file malware data mining

6. User dapat mengeksekusi file tersebut dengan mengatur ulang atau menghapusnya.

7. Aplikasi akan mendisplay untuk melakukan pilihan ya atau tidak untuk melanjutkan dan menghentikan aplikasi pendeteksi tersebut

Kekurangan : tingkat akurasi masih belum diketahui

Kelebihan : Source code lebih mudah di eksekusi.

3.2.4 Spesifikasi Sistem

Pada Tabel 3.2.4 adalah daftar kebutuhan perangkat keras

Perangkat keras	**Jumlah**	**Keterangan**
VGA card	1	Nvidia Geforce GT 630
Processor	1	Intel i5
Memory	1	8 GB Ram
System Type	1	64-bit Operating system,x64-operate based processor
Hard disk	1	1TB
Operating system	-	Windows 10

3.2.5 Perangkat Lunak

Pada Tabel 3.2.5 adalah daftar kebutuhan perangkat lunak

Perangkat Lunak	**Fungsi**
Go-lang	Mengeksekusi Program yang telah di rancang
Bracket	Mengubah atau membuat program sistem
Notepad++	Mengubah sebagian dari source code

BAB IV IMPLEMENTASI DAN PENGUJIAN

4.1 Implementasi

Dalam pembangunan Sistem ini hasil yang akan di tampilkan pada system ialah sebagai berikut :

1. Sistem dapat melakukan scanning pada file Enkripsi

2. Mendeteksi file malware pada setiap file ataupun folder

3. Memberikan notifikasi pada user jika terdeteksi malware

4. User dapat mengesekusi file tersebut dengan memberikan perintah pada aplikasi.

4.2.Pengujian

Dalam pengujian system ini terdapat beberapa source code yang akan di gunakan dalam melakukan scanning file ada tahapan nya sebagai berikut.

4.2.1 Pengujian pada Sistem

Tujuan utama pengujian pada Sistem adalah untuk memberikan hasil File scan

Pada pengujian ini merupakan source code Program dibuat untuk mendeteksi adanya injeksi malware terhadap file atau pun seluruh file dapat

```
#### Without repo cloned
Copy and paste these commands:

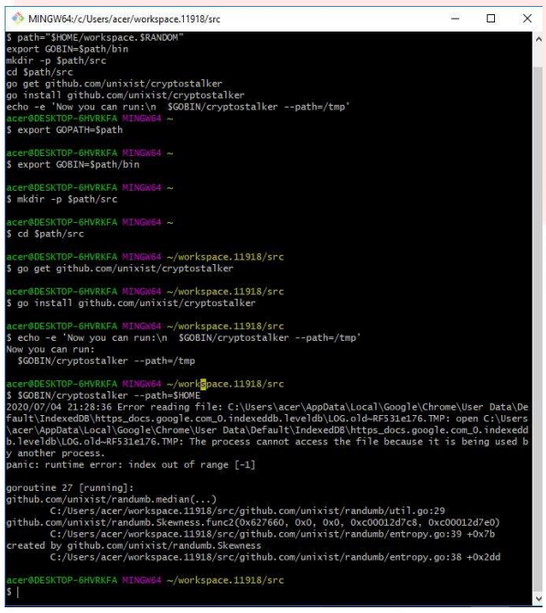
```bash
path="$HOME/workspace.$RANDOM"
export GOPATH=$path
export GOBIN=$path/bin
mkdir -p $path/src
cd $path/src
go get github.com/unixist/cryptostalker
go install github.com/unixist/cryptostalker
echo -e 'Now you can run:\n  $GOBIN/cryptostalker --path=/tmp'
```

Example
```

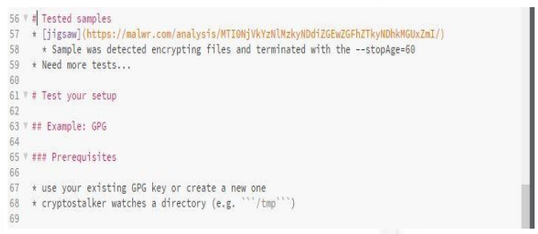
dilihat pada gambar 4.2.1

4.2.2 Skenario Pengujian pada Sistem

Pengujian pada Sistem yang akan dilakukan pada seluruh sistem seperti pada gambar 4.9.



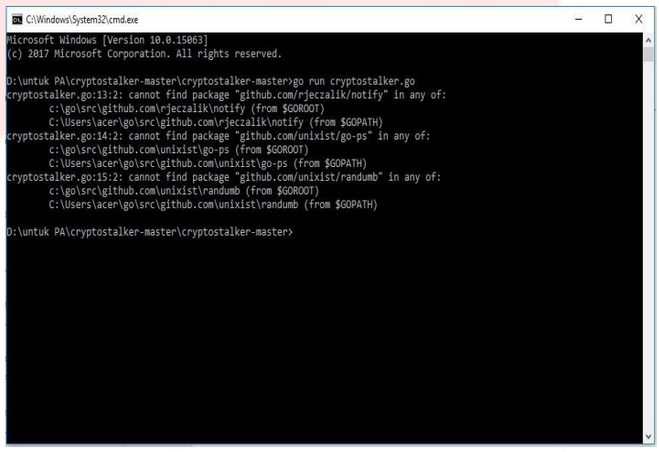
Kemudian menerapkan sample file yang ada pada source code di Bracket atau GO-lang



lalu fitur pada source code cukup memadai yang mana fitur di berlakukan ketika melakukan running program dan memberhentikan process scanning.

4.2.3 Pengujian pada Sistem yang dibangun

Program Pengujian pada Sistem yang dibangun Pada pengujian ini, Program dibuat untuk mendeteksi ada nya file yang akan terdeteksi malware maka dari itu Cryptostalker akan melakukan scanning seperti sistem saat ini.



.

BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari serangkaian pengujian yang dilakukan pada sistem yang dibangun dan pendeteksi, maka dapat disimpulkan bahwa :

1. Sistem dapat mendeteksi malware dengan menscanning seluruh folder yang di pilih atau di tetapkan.
2. Hasil scanning akan ternotifikasi jika file terinjeksi virus.
3. Tingkat keakurasian sistem yang dibangun yaitu 68%.

5.2 Saran

Untuk pengembangan lebih lanjut pada penelitian sistem ini, disarankan untuk:

1. Memaksimalkan tingkat keakurasian sistem saat ini.
2. Membuat system dapat mengeksekusi file yang terinjeksi malware.
3. Membuat rancangan yang lebih baik lagi dalam segi tampilan dan process.

DAFTAR PUSTAKA

[1] https://libraryeproceeding.telkomuniversity.ac.id/index.php/engineering/article/viewFile/9955 /981.

[2] https://tekno.tempo.co/read/1277229/microsoft-80-ribu-komputer-dibajak-malware-jaditambang-bitcoin/full&view=ok

[3] https://github.com/gsuareztangil/cryptomining-malware

[4] https://dailysocial.id/post/burger-king-indonesia-cryto-mining-malware-injection].

[5] https://www.dignited.com/45408/whats-crypto-mining-and-how-does-it-hurt-your-pc/

[6] https://www.logique.co.id/blog/2019/08/19/bahasa-pemrograman-golang/

[7] https://github.com/unixist/randumb.

[8] https://github.com/Joeyn414/cryptostalker.

[9] https://bagustris.github.io/shell-tutorial/02-filedir/.