Analisa *Malware* Menggunakan Metode *Dynamic Analysis* Pada Jaringan Universitas Sam Ratulangi

Virgiawan A. Manoppo, Arie S. M. Lumenta, Stanley D. S. Karouw
Jurusan Teknik Elektro, Universitas Sam Ratulangi Manado, Jl. Kampus Bahu, 95115, Indonesia
afidmanoppo@gmail.com, al@unsrat.ac.id, stanley.karouw@unsrat.ac.id
Diterima: tgl; direvisi: tgl; disetujui: tgl

***Abstract* — The globalization era brings exponential development to various sectors, one of which is the field of science and technology. Unfortunately, the development is not only on the positive aspect, but also spread to the negative direction. One example of the negative development of technology is the emergence of various kinds of cyber crime, such as the spread of malware. The purpose of this study is to analyze the characteristics of malware found on Sam Ratulangi University's network. The method used in this research is Dynamic Analysis using the Cuckoo Sandbox tool to prevent the infection of malware itself. After analyzing the characteristics of the malware, the researcher concluded that are several signatures, strings, and changes to the registry value.**

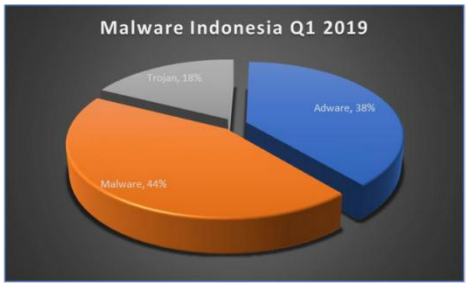
***Keywords* — Cuckoo Sandbox; Dynamic Analysis; Malware; Malware Analysis.**

***Abstrak* — The Di era globalisasi ini, terdapat berbagai macam sektor yang mengalami perkembangan yang eksponensial, salah satu di antaranya adalah bidang IPTEK. Sayangnya, perkembangan tersebut tidak hanya berdampak positif, tapi juga merambah ke arah negatif. Salah satu perkembangan negatif tersebut adalah munculnya berbagai macam tindak kejahatan siber, seperti penyebaran malware. Tujuan dari penelitian ini adalah untuk menganalisa karakteristik malware yang ditemukan pada jaringan Universitas Sam Ratulangi. Adapun metode yang dipakai dalam penelitian ini adalah dengan Dynamic Analysis dan menggunakan tool Cuckoo Sandbox, sehingga tidak ada resiko untuk terinfeksi malware. Berdasarkan analisa yang dilakukan tentang karakteristik dari malware, dapat disimpulkan bahwa terdapat beberapa signature, string, dan perubahan pada value registry.**

Kata kunci* — Analisa *Malware; Cuckoo Sandbox; Dynamic Analysis; Malware.

I. PENDAHULUAN

Pada era globalisasi saat ini, aktifitas sehari-hari manusia sudah bergantung dengan teknologi. Baik itu dalam bidang sosial, politik, ekonomi maupun pendidikan. Dalam dunia pendidikan, teknologi dimanfaatkan dengan berbagai macam cara, seperti penggunaan e-book, e-learning, website dan lain lain. Perkembangan teknologi ini tentu dimanfaatkan oleh berbagai pihak. Selain pemanfaatan dalam sisi positif, terdapat pula pihak-pihak yang memanfaatkan dalam sisi negatif. Dalam hal ini seperti mengembangkan sebuah software yang dapat melakukan tindak kejahatan atau yang biasa disebut cyber crime. Salah satu bentuk dari kejahatan ini yaitu penyebaran Malware dengan begitu mudah. Berdasarkan laporan dari situs Vaksin.com pada kuartal 1 tahun 2019 di dominasi oleh 3 kategori malware, pertama kategori malware sendiri (44 %) disusul oleh Adware (38 %) dan terakhir adalah Trojan (18 %).



Gambar 1.1 Statistik *Malware* Indonesia Kuartal 1 2019 (Sumber : www.vaksin.com)

Malicous software atau yang lebih dikenal sebagai Malware merupakan perangkat lunak yang secara eksplisit didesain untuk melakukan aktifitas berbahaya atau perusak perangkat lunak lainnya seperti Trojan, Virus, Spyware dan Exploit [2]. Sehingga dibutuhkan Analisa untuk menentukan apakah aplikasi dalam komputer itu teridentifikasi adalah sebuah Malware dan untuk mengetahui karakteristik dari malware tersebut dan dampak pada sistem setelah malware tersebut dieksekusi.

Berdasarkan fakta – fakta terkait malware di atas perlu dilakukan metode analisa untuk mengetahui motif – motif dari serangan malware sehingga kita mengetahui karakteristik dari malware tersebut.

Analisa malware secara umum dapat dilakukan dengan dua metode, yaitu Dynamic Analysis, dan Static Analysis [1]. Meskipun tujuan dari kedua metode tersebut sama yaitu untuk menjelaskan tentang bagaimana sebuah malware berkerja tetapi dalam proses analisa kedua metode tersebut sangatlah berbeda dalam segi tools, waktu dan kemampuan. Dynamic analysis dilakukan dengan mengeksekusi contoh malware untuk kemudian dipelajari perilaku yang ditimbulkan oleh malware tersebut. Berbeda dengan static analysis yang pada saat proses

analisanya tidak mengeksekusi contoh malware melainkan dengan membongkar source code malware lalu mempelajari dan memahami kode tersebut.

Dynamic Analysis bisa dilakukan dengan dua cara yaitu manual dan menggunakan tool analisa otomatis yaitu cuckoo sandbox. Cuckoo sandbox dapat melakukan analisa malware secara otomatis dan menampilkan informasi – informasi yang dilakukan oleh sampel malware.

A. *Malware*

Malware (Malicious Software) merupakan program yang dirancang untuk disusupkan ke dalam sebuah sistem dengan tujuan untuk melakukan beraneka ragam aktivitas yang bersifat merugikan pemiliknya. Merugikan dalam arti kata dampak negatif yang ditimbulkan dapat berkisar mulai dari sekedar memperlambat kinerja sistem hingga merusak bahkan menghancurkan data penting yang tersimpan dalam sistem yang dimaksud. Ada tiga jenis Malware klasik yang paling banyak ditemui, yaitu: Virus, Worms, dan Trojan Horse. (Indrajit, 2011).

1. *Virus*

Virus merupakan program komputer yang bersifat "*malicious*" (memiliki tujuan merugikan maupun bersifat mengganggu pengguna sistem) yang dapat menginfeksi satu atau lebih sistem komputer melalui berbagai cara penularan yang dipicu oleh otorasisasi atau keterlibatan "user" sebagai pengguna komputer.

2. *Worms*

Worms merupakan program yang dibangun dengan algoritma tertentu sehingga yang bersangkutan mampu untuk mereplikasikan dirinya sendiri pada sebuah jaringan komputer tanpa melalui intervensi atau bantuan maupun keterlibatan pengguna.

3. *Trojan Horse*

Trojan Horse merupakan program *malicious* yang dimasukkan ke dalam sistem melalui sebuah program atau aktivitas yang legal – seperti: melalui proses instalasi perangkat lunak aplikasi, melalui proses "upgrading" versi software yang baru, melalui proses "download" program - program freeware, melalui file - file multimedia (seperti gambar, lagu, dan video), dan lain sebagainya.

B. Model Analisa *Malware*

Pada dasarnya malware adalah sebuah program, yang disusun berdasarkan tujuan tertentu dengan menggunakan logika dan algoritma yang relevan dengannya. Oleh karena itulah maka model analisa yang biasa dipergunakan untuk mengkaji malware sangat erat kaitannya dengan ilmu dasar komputer, yaitu: bahasa pemrograman, algoritma, struktur data, dan rekayasa piranti lunak.

Secara umum, ada 3 (tiga) jenis analisa terhadap sebuah program untuk mendeteksi apakah yang bersangkutan merupakan malware atau bukan. Ketiga pendekatan dimaksud akan dijelaskan dalam masing - masing paparan sebagai berikut [4]:

1. *Surface Analysis*

Sesuai dengan namanya, "surface analysis" adalah suatu kajian pendeteksian malware dengan mengamati sekilas ciri - ciri khas sebuah file program tanpa harus mengeksekusinya. Untuk melihat ciri khas tersebut dapat dilakukan dengan menggunakan bantuan software atau perangkat aplikasi pendudukung.

2. *Runtime Analysis*

Pada dasarnya ada kesamaan antara runtime analysis dengan surface analysis, yaitu keduanya sama - sama berada dalam ranah mempelajari ciri - ciri khas yang selayaknya ada pada sebuah program yang normal. Bedanya adalah bahwa dalam runtime analysis, dipersiapkan sebuah prosedur dan lingkungan untuk mengeksekusi atau menjalankan program yang dicurigai mengandung atau sebagai malware tersebut.

Model analisa ini menghasilkan kajian yang lebih mendalam karena selain dihilangkannya proses "menduga - duga", dengan mengeksekusi malware dimaksud akan dapat dilihat "perilaku" dari program dalam menjalankan "skenario jahatnya" sehingga selanjutnya dapat dilakukan analisa dampak terhadap sistem yang ada.

3. *Static Analysis*

Dari ketiga metode yang ada, static analysis merupakan model kajian yang paling sulit dilakukan karena sifat analisanya yang "white box" alias pengkajian melibatkan proses melihat dan mempelajari isi serta algoritma program malware dimaksud, sambil mengamati sekaligus menjalankan/mengeksekusinya.

Karena sifat dan ruang lingkupnya yang cukup luas dan mendalam, strategi khusus perlu dipersiapkan untuk melakukan kajian ini. Disamping itu, kajian ini juga memerlukan sumber daya yang khusus – misalnya adalah SDM yang memiliki pengetahuan dan pengalaman dalam membuat serta membaca program berbahasa mesin atau rakitan (assembly language) serta ahli arsitektur dan organisasi piranti komputasi seperti komputer, PDA, tablet, mobile phone, dan lain sebagainya.

4. *Dynamic Analysis*

Analisis Dinamis dilakukan dengan menjalankan sampel malware pada sebuah ruang lingkup yang dikontrol dan dimonitor selama ia berjalan. Pada beberapa kasus, analisis statis tidak menampilkan informasi yang banyak dikarenakan obfuscation, dan packing. Pada kasus seperti ini, Analisis Dinamis adalah cara terbaik untuk mengidentifikasi fungsionalitas malware. Berikut adalah langkah –langkah [5].

C. *Cuckoo Sandbox*

Cuckoo Sandbox merupakan tool analisa malware dan dapat memberikan beberapa informasi mengenai malware yang sedang berjalan dalam lingkungan yang terisolasi [3].

Hal yang dapat dilakukan Cuckoo sandbox adalah sebagai berikut:

1. *Native functions* dan *Windows API Calls Trace* yang dapat mencatat setiap eksekusi kode dari suatu file yang diupload ke dalam *Cuckoo Sandbox*.

2. Melakukan pencatatan pada setiap *file* yang dibuat atau dihapus dari sistem.

3. *Memory dump* dari hasil analisis *malware*.

4. Jejak aliran jaringan dalam format PCAP.

5. *Screenshot desktop* selama aktivitas analisis *malware* berlangsung.

6. *Full memory dump* dari mesin VM.

Cuckoo Sandbox dapat melakukan analisa terhadap berbagai macam sampel malware. Beberapa jenis file yang dapat dianalisa dengan Cuckoo adalah sebagai berikut.

1. File .exe *(Generic Windows Executable)*
2. File DLL
3. Dokumen PDF
4. Dokumen *Microsoft Office*
5. Halaman Web
6. *Script PHP*

Setelah dijalankan, Cuckoo melaporkan hasil analisa malware. Hasil analisa yang dilaporkan antara lain :

1. API calls yang dijalankan malware.
2. *File* yang dibuat.
3. *File* yang dihapus.
4. *File* yang diunduh *malware.*
5. Aktivitas *malware* di *memory (memory dumps)*
6. Trafik jaringan yang diakses *malware* (dalam format PCAP).

D. Penelitian Terkait

Analisa Malware Trojan. Sulhaedir. Teknik Informatika (2016). Penelitian ini membahas tentang analisa malware trojan menggunakan analisa static dan dinamis. Hubungan dengan peneltian ini adalah kesepahaman dalam konsep metode static analisys untuk melakukan analisa malware, sedangkan perbedaan dengan penelitian ini adalah aplikasi yang terduga malware telah diketahui karakteristik malware trojan pada penelitian saya belum diketahui.

Analisis Malware Dengan Teknik Static Analysis (Irman Hariman,Azhar,Syams). Penelitian ini membahas tentang analisa malware worm menggunakan metode static analysis dan cara mencegah agar malware tidak berkembang biak dan pembuatan aplikasi antimalware. Hubungan dengan penelitian ini adalah kesepahaman konsep tentang metode static analysis, sedangkan perbedaan dengan penelitian ini adalah aplikasi yang terduga malware telah diketahui karakteristik malware worm dan pembuatan aplikasi antimalware pada penelitian saya belum diketahui.

Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis (Triawan Adi Cahyanto). Penelitian ini membahas tentang analisa malware posion ivy RAT (Remote Access Trojan) yang menggunakan metode static dan dinamis untuk mengetahui output dari kedua metode ini sama. Hubungan dengan metode ini adalah kesepahaman tentang konsep static analysis yang digunakan untuk mengidentifikasi malware poison ivy RAT

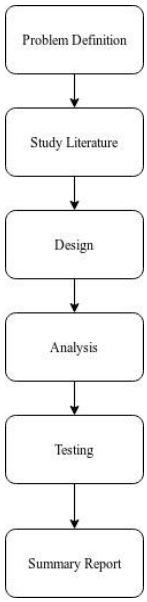
Malware Analysis on Windows Operation System to Detect Trojan. Sabam Chandra Yohanes Hutauruk, Fazmah Arif Yulianto, Gandeva Bayu Satrya. Penelitian ini membahas tentang analisa malware trojan menggunakan metode static dan dinamis pada sistem operasi windows. Hubangan dengan penelitian ini adalah kesepahaman konsep static analysis untuk mengetahui karakteristik dari sebuah malware.

Pembangunan Server Analisis Malware menggunakan Cuckoo Sandbox pada Sistem Operasi berbasis Linux. Rida Firana, Setia Juli Irzal Ismail, Periyadi. Penelitian ini membahas tentang analisa malware menggunakan metode dinamis dan mempunyai kesamaan tools untuk melakukan analisa yaitu Cuckoo Sandbox.

II. METODE

A. Tahapan Penelitian

Pada bagian ini menjelaskan mengenai tahapan penelitian yang digunakan untuk menganalisa malware [3].



Gambar 2.1 Tahapan Penelitian

1. *Problem Definition*

Pada tahap ini penulis mengidentifikasi masalah yang dibahas dalam penelitian, latar belakang maupun batasan masalah yang digunakan.

2. *Study Literature*
Pada tahap ini penulis mempelajari literatur yang berhubungan dengan penelitian, seperti literatur mengenai malware dan teknik analisis malware, cuckoo sandbox. Literatur yang diperoleh berupa dokumentasi penelitian – penelitian sebelumnya seperti jurnal, paper, serta website yang terpercaya.

3. *Design*
Pada tahap ini penulis melakukan perancangan sistem yang meliputi tahapan penelitian dan lingkungan yang akan digunakan untuk proses analisa malware.

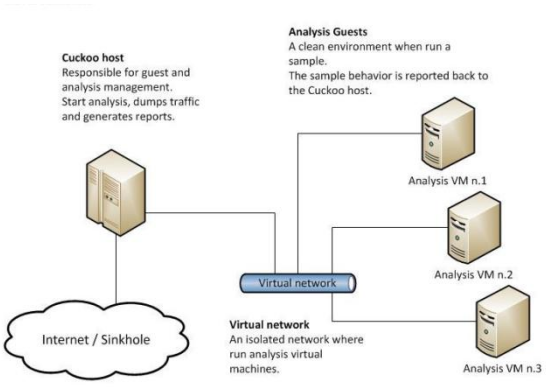
4. *Analysis*
Pada tahap ini penulis melakukan analisis terhadap sampel file malware, tools, Data yang digunakan adalah data sampel malware yang diambil pada website universitas sam ratulangi. Tools yang dipakai adalah Cuckoo SandBox untuk proses analisa dinamik.

5. *Testing*
Pada tahap ini penulis mengeksekusi malware menggunakan tool cuckoo sandbox dan mengamati segala aktvitas yang dilakukan oleh malware.

6. *Summary Report*
Pada tahap ini penulis mengevaluasi keseluruhan tahapan penelitian dan mendokumentasikan dalam bentuk laporan.

B. Arsitektur Sistem

Desain sistem yang digunakan dapat dilihat pada gambar berikut.



Gambar 2.2 Arsitektur sistem
(Sumber:https://medium.com/@warunikaamali/cuckoo-sandbox-installation-guide-d7a09bd4ee1f)

Arsitektur Cuckoo Sandbox terdiri dari sebuah pusat manajemen perangkat lunak yang menangani eksekusi sampel malware dan analisis malware. Tiap analisis dijalankan di dalam sebuah mesin virtual yang terisolasi (dari jaringan luar). Infrastruktur cuckoo tersusun dari sebuah mesin host dan beberapa mesin guest.

Mesin host menjalankan komponen inti dari sandbox yang mengelola seluruh proses analisis, sedangkan mesin guest adalah lingkungan yang terisolasi dimana sampel malware dengan aman untuk proses analisis

C. Rencana Pengerjaan.

Hal yang akan dilakukan untuk membangun lingkungan isolasi (virtual machine) diantaranya :

1) Instalasi sistem operasi linux Mint 19.3 pada server host.

2) Instalasi software yang dibutuhkan pada host seperti package. dependencies dan libraries untuk cuckoo sandbox, cuckoo sandbox 2.0.7 dan Virtualbox 6.0.

3) Pembuatan mesin Virtual yang berperan sebagai guest atau ruang lingkup pengujian sampel malware. Sistem operasi yang digunakan sebagai guest adalah Windows 7 SP3 32bit.

4) Pembuatan folder sharing antara server host dan mesin virtual.

5) Konfigurasi server host meliputi konfigurasi file cuckoo sandbox (versi 2.0.7), konfigurasi Virtualbox dan konfigurasi iptables server host. Pengaturan iptables dibuat untuk mengatur IP Forwarding dan filtering mesin virtual.

6) Konfigurasi mesin virtual meliputi instalasi aplikasi python, python imaging Library, Agent.py, dan aplikasi lain yang biasa dipakai pada personal komputer asli.

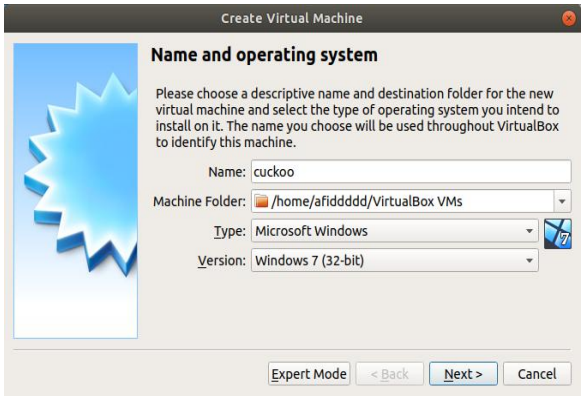
III. HASIL DAN PEMBAHASAN

A. Implementasi

Pada tahap ini menjelaskan tentang pembangunan server analisa malware meliputi konfigurasi Virtualbox 6.0, instalasi Cuckoo Sandbox 2.0.7, package dependencies, mesin virtual dan konfigurasi seluruh sistem.

1. Konfigurasi Virtualbox
Untuk melakukan analisa malware dengan metode dinamik kita perlu lingkungan yang aman (terisolasi) dari komputer host dimana malware akan dijalankan. Didalam virtualbox kita akan membuat mesin virtual atau guest dengan sistem operasi windows 7 sp1.

p-ISSN : 2301-8402, e-ISSN : 2685-368X ,dapat diakses melalui https://ejournal.unsrat.ac.id/index.php/elekdankom



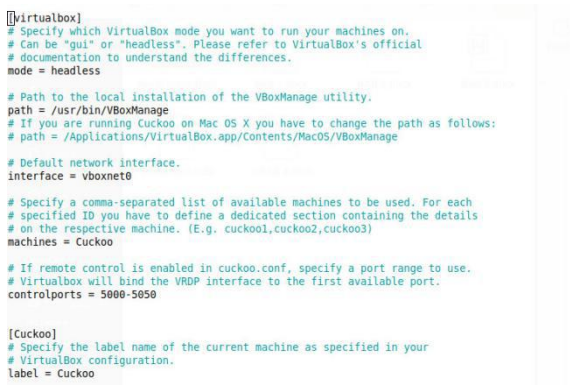
Gambar 3.1 Proses Konfigurasi Virtualbox

2. *Instalasi Package Dependencies dan Cuckoo Sandbox.*

Cuckoo Sandbox merupakan aplikasi yang sangat modular sehingga membutuhkan package dan libraries untuk menjalankan setiap syntax-nya. Instalasi dilakukan via Terminal Linux Mint.

3. *Konfigurasi Cuckoo Sandbox*

Setelah semua ter-install perlu melakukan konfigurasi pada aplikasi cuckoo sandbox agar bisa saling terkoneksi. Konfigurasi dilakukan via terminal linux.



```
[virtualbox]
# Specify which VirtualBox mode you want to run your machines on.
# Can be "gui" or "headless". Please refer to VirtualBox's official
# documentation to understand the differences.
mode = headless

# Path to the local installation of the VBoxManage utility.
path = /usr/bin/VBoxManage
# If you are running Cuckoo on Mac OS X you have to change the path as follows:
# path = /Applications/VirtualBox.app/Contents/MacOS/VBoxManage

# Default network interface.
interface = vboxnet0

# Specify a comma-separated list of available machines to be used. For each
# specified ID you have to define a dedicated section containing the details
# on the respective machine. (E.g. cuckoo1,cuckoo2,cuckoo3)
machines = Cuckoo

# If remote control is enabled in cuckoo.conf, specify a port range to use.
# Virtualbox will bind the VRDP interface to the first available port.
controlports = 5000-5050


[Cuckoo]
# Specify the label name of the current machine as specified in your
# VirtualBox configuration.
label = Cuckoo
```

Gambar 3.2 Konfigurasi Cuckoo Sandbox ke Virtualbox

B. Pengujian

Pada tahap ini kita mulai menguji cuckoo sandbox dan file malware untuk proses analisa dinamik dan melihat karakteristik dari malware tersebut.

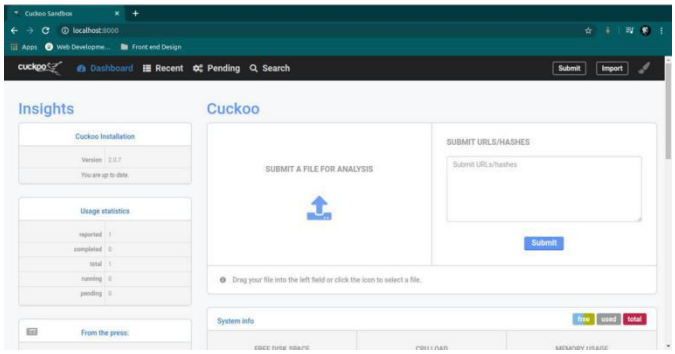
1) Gambar 3.3
Merupakan proses menjalankan *Cuckoo Sandbox* via terminal Linux.
2) Gambar 3.4
Merupakan tampilan utama *Cuckoo Sandbox* digunakan untuk mengupload sampel *malware.*
3) Gambar 3.5
Meruapakan tampilan ketika sampel malware telah dimasukkan/diupload kedalam *Cuckoo Sandbox.*
4) Gambar 3.6
Merupakan analisa *Cuckoo Sandbox* yang menampilkan hasil *strings.*
5) Gambar 3.7
Merupakan analisa *Cuckoo Sandbox* menampilkan sampel *malware* yang menjalankan *file wscript.exe*
6) Gambar 3.8
Merupakan tampilan dimana sampel malware melakukan duplikasi diri.
7) Gambar 3.9
Merupakan tampilan dimana *malware* mengakses diri sendiri.
8) Gambar 3.10
Merupakan tampilan dimana *malware* melakukan perubahan value registry :
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\Levels
9) Gambar 3.11
Merupakan tampilan dimana *malware* melakukan akses ke *registry :*
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\Levels

Tabel 3.1 Informasi *File Malware*

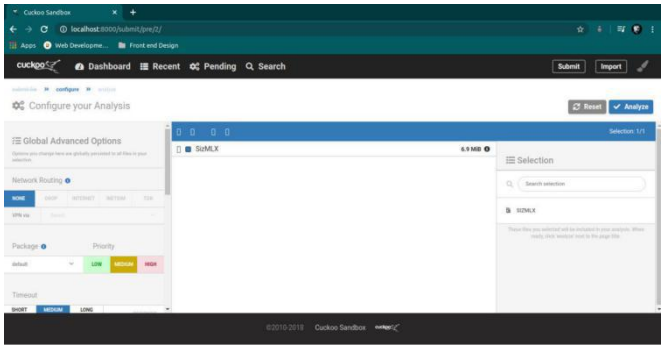
File Name	*SizMLX*
File Size	6.9MB
File Type	*PHP script, ASCII text, with very long linesELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, stripped*
MD5	5447cf2d4b1f61ed74d254c48461a08a
SHA1	5dbd07809d224103d87518521449f6344f04c38c
SHA256	0bf7c36ec904a63d6a567f19998f34c321e1905b4c5548731e9cc2886b236703
SHA512	efba09307ec8b95c693004dc7186bae151a46fcdb8495c3620e5383fd2b351de94a55635524219e77816625b6169be7a501a4fca9325d0c7b9a7f74a87a6a9f8
CRC32	912DED40
ssdeep	98304:lbqAyMjk9vhqo3UMK24CpIscr/eMj2WIX:FLyMw7qo9mtjf1
Yara	- embedded_pe - Contains an embedded PE32 file - embedded_win_api - A non-Windows executable contains win32 API functions names

```
afiddddd@afiddddd:~$ cd .cuckoo
afiddddd@afiddddd:~/.cuckoo$ cuckoo -d
```


Gambar 3.3 Proses Menjalankan Cuckoo Sandbox



Gambar 3.4 Halaman Utama Cuckoo Sandbox

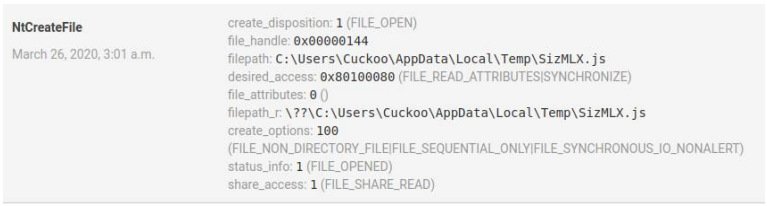


Gambar 3.5 Proses Upload Sampel Malware ke Cuckoo Sandbox

```
MoYxxE1lw1fXwbYVoYL-/Y7K8RnoD_Y5azr-Ujwqv/qoUaxXZH0mAD2v_3m_OC/M9vODtAusDYIWS2Xellb
singu?
runtu/
tX;ChuY
|$$9;u
|$D9;u
2006u1
2006u5
=WITAt
|$H9;u
|$L9;u
|$09;u
|$89;u
|$09;u
|$$9;u
|$$9;u
|$09;u
|$(9;u
|$,9;u
|$ 9;u
|$D9;u
|$@9;u
|$,9;u
|$,9;u
|$,9;u
|$H9;u
```

Gambar 3.6 *Strings* dari sampel malware

Gambar 3.7 *Sampel Malware Menjalankan wscript.exe*



Gambar 3.8 Sampel Melakukan Duplikat

Gambar 3.9 Sampel Mengakses Diri Sendiri

Gambar 3.10 Sampel Melakukan Perubahan Value Registry

Gambar 3.11 Sampel Mengakses Registry

C. Summary Result

Berikut adalah beberapa signatures summary yang menunjukkan perilaku sampel A-W ketika dijalankan pada ruang lingkup mesin virtual.

Tabel 3.2 *Signatures*

Engine	Mesin Virtual	Sampel	Signatures
Cuckoo Sandbox	*Windows 7 SP1*	*A-W*	Membaca data *image binary* milik dirinya sendiri
			Melakukan beberapa *request UDP*
			Menambahkan *value* pada beberapa *registry*
			Teridentifikasi sebagai *malware* oleh 35 dari 57 *Antivirus* pada *VirusTotal*
			Terdapat anomali – anomali karakteristik biner

Tabel 3.3 *Summary Signatures*

Engine	Mesin Virtual	Sampel	Malscore	Kategori Malscore	Virustotal Ratio	Definisi Virustotal Ratio	Jenis Malware
Cuckoo Sandbox	*Windows 7 SP1*	*A-W*	37	Malicious	35/57	67% Terdeteksi sebagai *malware*	*Trojan*

IV. KESIMPULAN DAN SARAN

A. *Kesimpulan*

Berdasarkan penelitian ynag sudah dilakukan untuk menganalisis karakteristik dari sampel malware yang diperoleh dari jaringan universitas sam ratulangi maka kesimpulan dari tugas akhir ini adalah :

1) Metode dynamic analysis dapat mempermudah kita untuk analisa malware karena kita menjalankan malware tersebut dilingkungan yang terisolasi.

2) Hasil analisa malware menggunakan tool cuckoo sandbox yang didapatkan adalah informasi malware, karakteristik dari malware, behaviour analysis, static analysis dan tingkat maliciousness malware berdasarkan hasil yang di dapat dari VirusTotal.

B. *Saran*

1) Untuk penelitian berikutnya diperlukan pemahaman analisa malware menggunakan metode static analysis agar informasi lebih mendalam mengenai karakteristik malware bisa didapatkan.

2) Untuk penelitian berikutnya dapat dilakukan pada platform selain windows dan linux, misalnya MacOS atau Android.

V. KUTIPAN

[1] Cahyanto, T. A., Wahanggara V., Ramadana D. 2017. "*Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis" Jurnal Sistem & Teknologi Informasi Indonesia, Vol. 2, No. 1.* Referensi : http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO/article/view/1037

[2] Kramer, S., & Bradfield, J. C. 2010 "*A general definition of malware"* Journal in Computer Virology. Referensi : https://link.springer.com/article/10.1007%2Fs11416-009-0137-1

[3] Sibarani, F. R., Sibuea, C. A., Situmorang, P. A. 2019 "*Pendekteksian Malware Dengan Menggunakan Analisis Dinamik Terhadap Aktivitas Jaringan".* Referensi : http://ri.del.ac.id:8080/xmlui/handle/123456789/429

[4] Indrajit, R. E. 2011. *"Pengantar Konsep Keamanan Informasi di Dunia Siber"* APTIKOM. Jakarta.

[5] Firana, R., Ismail, S. J. I., Periyadi. 2016. *"Pembangunan Server Analisis Malware Menggunakan Cuckoo Sandbox Pada Sistem Operasi Berbasis Linux".* Bandung: Universitas Telkom.

[6] Amali, W. "*Cuckoo Sandbox Installation Guide"* Medium, 9 Juli 2017. [Online]. Available: https://medium.com/@warunikaamali/cuckoo-sandbox-installation-guide-d7a09bd4ee1f