

**ANALISIS DAN DETEKSI MALWARE TROJAN PADA
BERKAS DOC MENGGUNAKAN METODE STATIS DAN
DINAMIS**

SKRIPSI



Disusun oleh:

**Samuel Sinambela
17.83.0050**

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021**

**ANALISIS DAN DETEKSI MALWARE TROJAN PADA
BERKAS DOC MENGGUNAKAN METODE STATIS DAN
DINAMIS**

SKRIPSI

Diajukan kepada Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
untuk memenuhi salah satu syarat memperoleh gelar Sarjana Komputer
Pada Jenjang Program Sarjana – Program Studi Teknik Komputer



Disusun oleh:

Samuel Sinambela
17.83.0050

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021**

HALAMAN PERSETUJUAN

SKRIPSI

**ANALISIS DAN DETEKSI MALWARE TROJAN PADA
BERKAS DOC MENGGUNAKAN METODE STATIS DAN
DINAMIS**

yang dipersiapkan dan disusun oleh

Samuel Sinambela

17.83.0050

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 4 Desember 2021

Dosen Pembimbing,

Wahyu Sukestyama Putra, S.T., M.Eng.

NIK. 190302328

HALAMAN PENGESAHAN
SKRIPSI
ANALISIS DAN DETEKSI MALWARE TROJAN PADA BERKAS DOC
MENGGUNAKAN METODE STATIS DAN DINAMIS

yang dipersiapkan dan disusun oleh

Samuel Sinambela

17.83.0050

Telah dipertahankan di depan Dewan Penguji
pada tanggal 21 Desember 2021

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Donni Prabowo, M.Kom.
NIK. 190302253

Majid Rahardi, S.Kom., M.Eng.
NIK. 190302393

Wahyu Sukestvama Putra, S.T., M.Eng.
NIK. 190302328

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 21 Desember 2021

DEKAN FAKULTAS ILMU KOMPUTER

Hanif AlFatta, M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Samuel Sinambela
NIM : 17.83.0050

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis dan Deteksi Malware Trojan pada Berkas Doc Menggunakan Metode Statis dan Dinamis

Dosen Pembimbing : Wahyu Sukestyama Putra, S.T., M.Eng.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 4 Desember 2021

Yang Menyatakan,

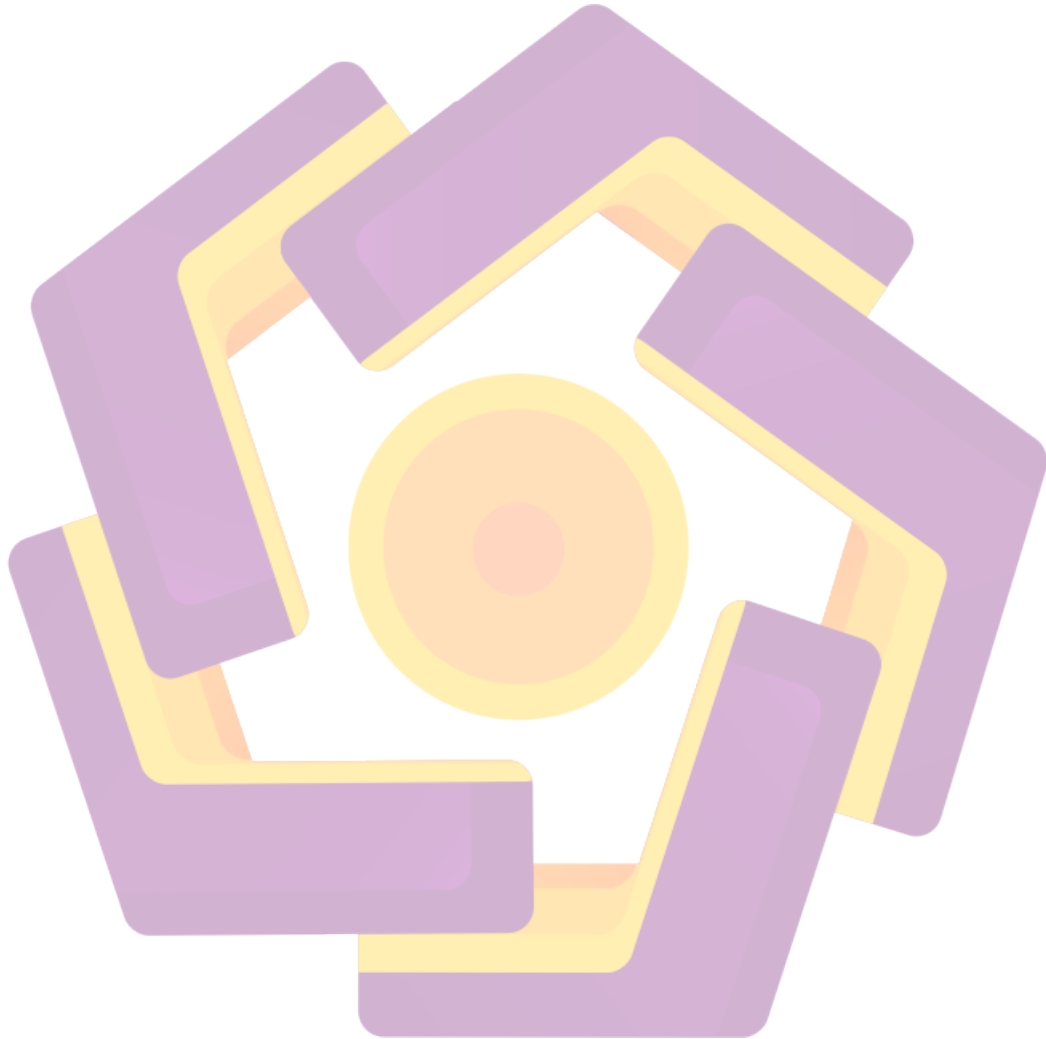


Samuel Sinambela

HALAMAN MOTTO

“Habis gelap, terbitlah terang”
(**Kartini**)

“Ketahuilah: Anda bisa memulai setiap pagi”
(**Tyler Joseph**)



HALAMAN PERSEMBAHAN

Puji syukur saya panjatkan ke hadirat Tuhan Yang Maha Esa, atas kasihnya sehingga skripsi ini selesai dengan sebaik-baiknya. Skripsi ini saya persembahkan untuk:

1. Kedua orang tua, Bapak Mohbin Sinambela dan Ibu Orlide Sumihar Sunggul Situmorang yang selalu mendoa'kan, memberi dukungan, dan bekerja keras demi masa depan saya.
2. Bapak Wahyu Sukestyama Putra, S.T., M.Eng. selaku dosen pembimbing yang telah membantu dalam penyusunan skripsi ini.
3. Kepada saudara-saudari saya yang selalu mendoa'kan, memberi semangat dan dukungan kepada saya.
4. Kepada seseorang yang sangat berharga bagi saya, Imelda Juliana Waruwu yang selalu mendoa'kan, menemani, dan memberi semangat kepada saya.
5. Kepada sahabat dan teman-teman yang ada disaat suka maupun duka selama masa perkuliahan saya.

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa atas berkat, kasih karunia, dan penyertaan-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul “Analisis dan Deteksi Malware Trojan pada Berkas Doc Menggunakan Metode Statis dan Dinamis”. Skripsi ini disusun sebagai syarat memperoleh gelar Sarjana Komputer pada program Studi S1 Teknik Komputer Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

Penulis menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, skripsi ini tidak mungkin dapat terselesaikan. Oleh karena itu, penulis menyampaikan terima kasih kepada:

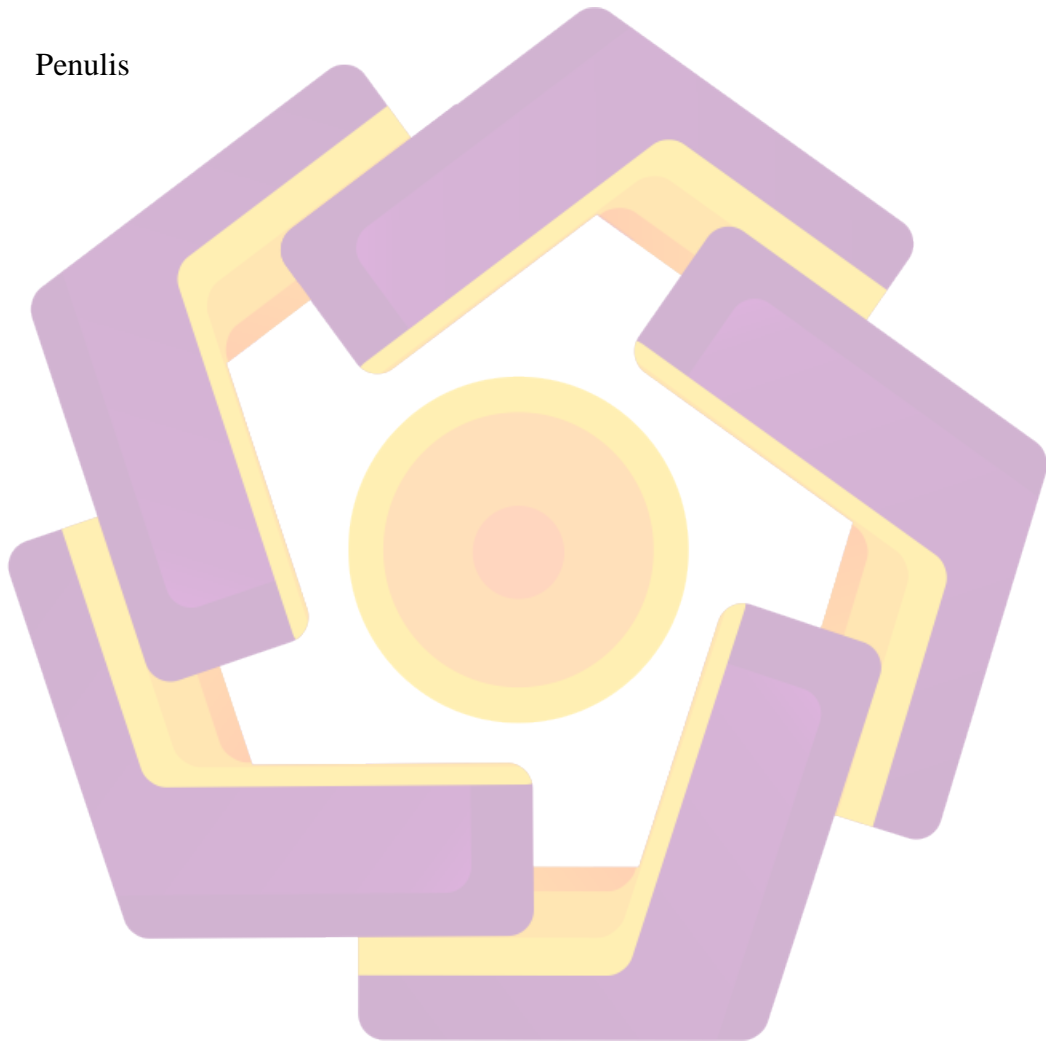
1. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas AMIKOM Yogyakarta.
2. Bapak Dony Ariyus, M. Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta.
3. Bapak Wahyu Sukestyama Putra, S.T., M.Eng. selaku Dosen Pembimbing yang telah bersedia memberikan pengarahan dan bimbingan dalam penyusunan Skripsi ini.
4. Seluruh Dosen, Staff, dan Karyawan Universitas AMIKOM Yogyakarta yang telah memberikan ilmu kepada penulis pada saat perkuliahan dan juga membantu penulis dalam kelancaran administrasi sampai terselesaikannya Skripsi ini.
5. Orang tua dan saudara-saudari yang selalu mendoakan dan memberikan dukungan penuh kepada penulis.
6. Serta kepada semua pihak yang telah membantu dalam penyusunan Skripsi ini yang tidak dapat penulis sebutkan satu per satu.

Penulis menyadari bahwa skripsi ini masih banyak kekurangan karena pengetahuan dan pengalaman yang terbatas, maka penulis mengharapkan kritik

dan saran yang membangun dari pembaca guna menyempurnakan skripsi ini.
Semoga skripsi ini memberikan manfaat bagi semua pihak.

Yogyakarta, 4 Desember 2021

Penulis

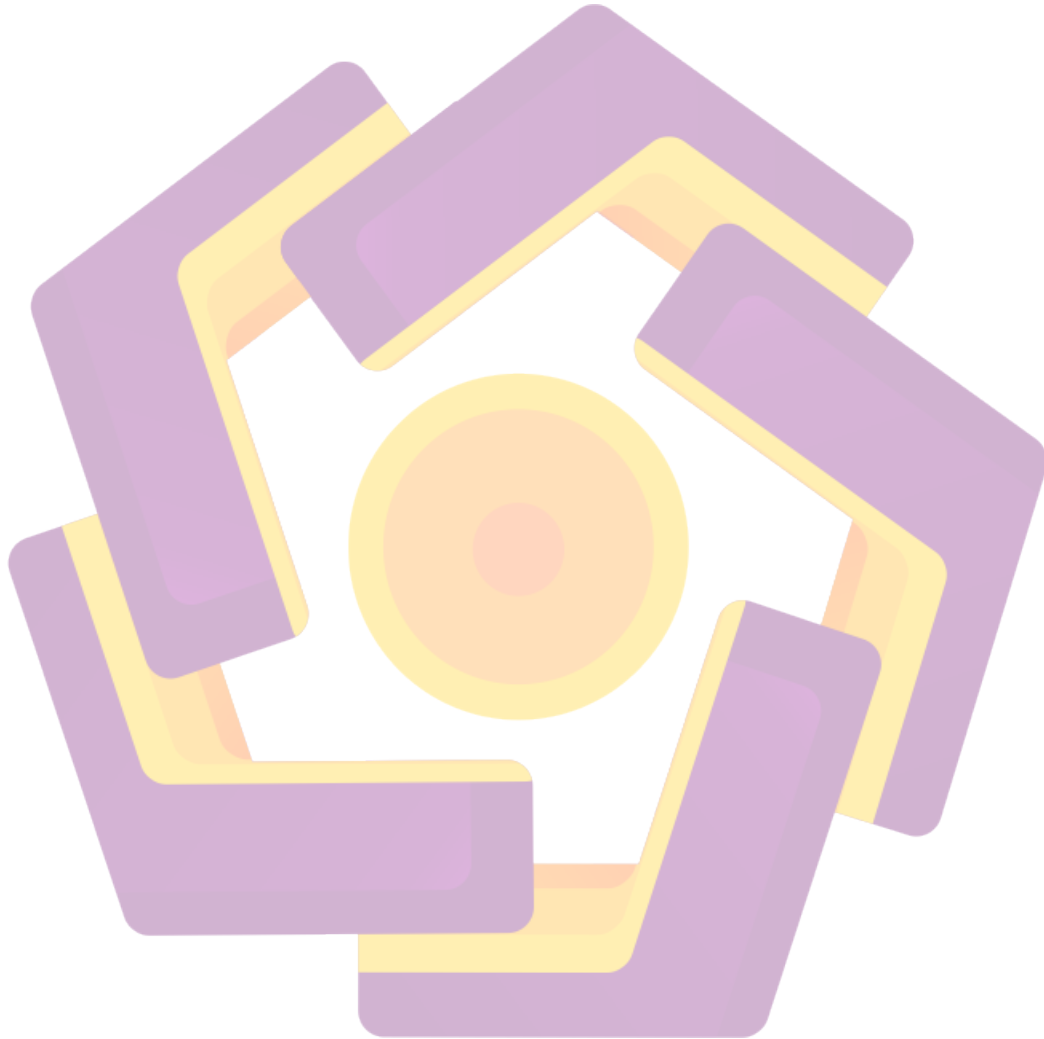


DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	v
HALAMAN MOTTO	ivi
HALAMAN PERSEMBAHAN.....	vii
KATA PENGANTAR	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xiv
INTISARI.....	xvi
<i>ABSTRACT</i>	xvii
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	3
1.5 Metode Penelitian	3
1.6 Sistematika Penulisan	4
BAB II LANDASAN TEORI	5
2.1 Tinjauan Pustaka.....	5
2.2 <i>Malware</i>	7
2.2.1 Virus	7
2.2.2 <i>Worm</i>	8
2.2.3 <i>Trojan</i>	8
2.2.4 <i>Adware</i>	8
2.2.5 <i>Spyware</i>	8
2.2.6 <i>Rootkit</i>	8
2.2.7 <i>Ransomware</i>	8
2.2.8 <i>Backdoor</i>	9

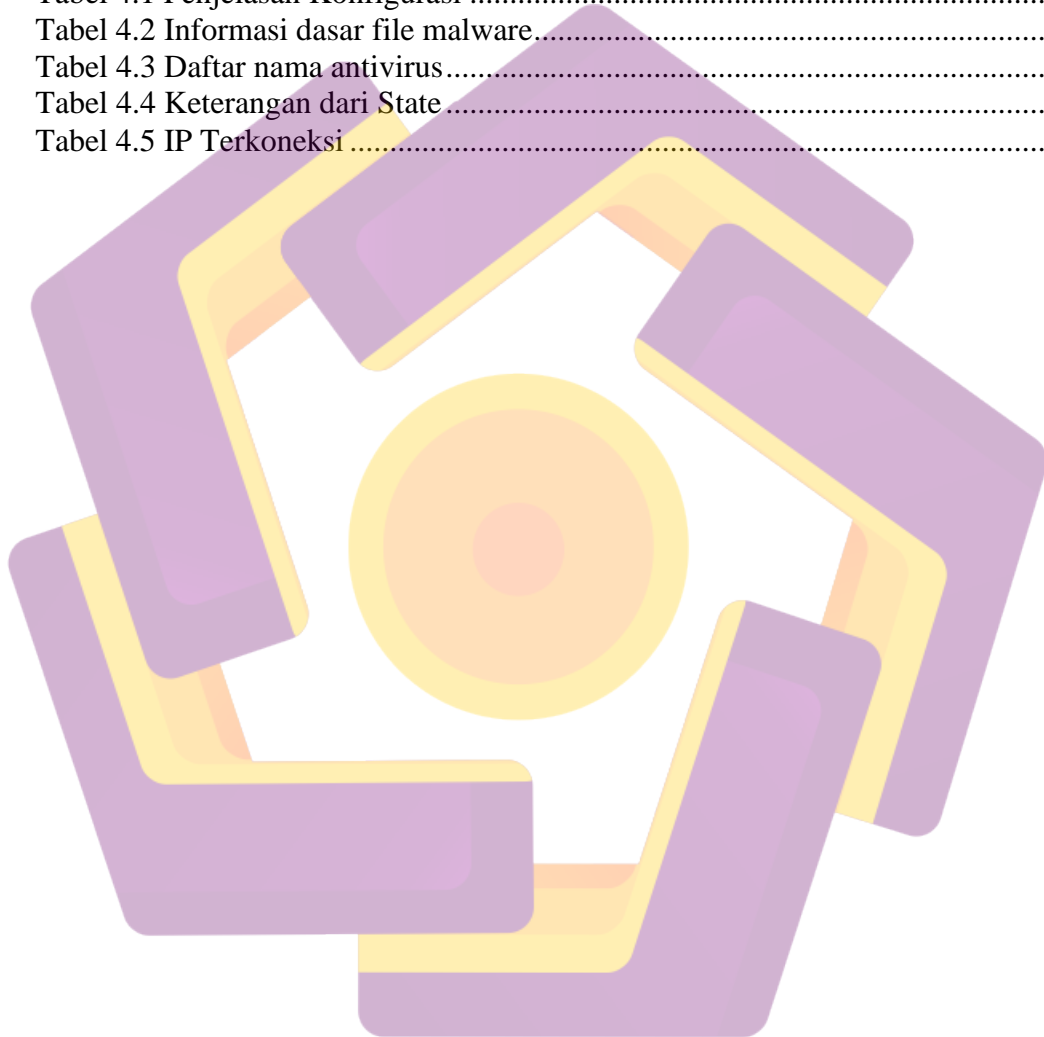
2.2.9 <i>Botnet</i>	9
2.3 <i>Macro Microsoft Office</i>	9
2.4 <i>Malware Macro</i>	9
2.5 <i>Antivirus</i>	9
2.6 <i>Metode Analisis Malware</i>	10
2.6.1 <i>Malware Analisis Statis</i>	10
2.6.2 <i>Malware Analisis Dinamis</i>	10
2.7 <i>VirusTotal</i>	10
2.8 <i>Anyrun</i>	10
2.9 <i>Kali Linux</i>	11
2.10 <i>Windows 7</i>	11
2.11 <i>Virtual Machine</i>	11
2.12 <i>Metasploit Framework</i>	11
2.13 <i>Payload</i>	11
2.13 <i>Meterpreter</i>	12
2.13 <i>Command Prompt</i>	12
2.13 <i>Task Manager</i>	12
BAB III METODOLOGI PENELITIAN	13
3.1 <i>Gambaran Umum Penelitian</i>	13
3.2 <i>Analisis dengan VirusTotal</i>	14
3.3 <i>Analisis dengan AnyRun</i>	15
3.4 <i>Alat dan Bahan Penelitian</i>	16
3.4.1 <i>Perangkat Keras</i>	16
3.4.2 <i>Perangkat Lunak</i>	16
3.4.3 <i>Tools Pendukung</i>	17
BAB IV PEMBAHASAN	19
4.1 <i>Pembuatan Malware Word</i>	19
4.2 <i>Analisis Statis</i>	22
4.2.1 <i>Analisis VirusTotal</i>	22
4.3 <i>Analisis Dinamis</i>	28
4.3.1 <i>Running Malware</i>	28
4.3.2 <i>Pendeteksian</i>	33

4.3.3 Analysis AnyRun.....	40
4.3.4 IP Penyerang.....	43
BAB V PENUTUP.....	49
5.1 Kesimpulan	49
5.2 Saran	50
DAFTAR PUSTAKA	51



DAFTAR TABEL

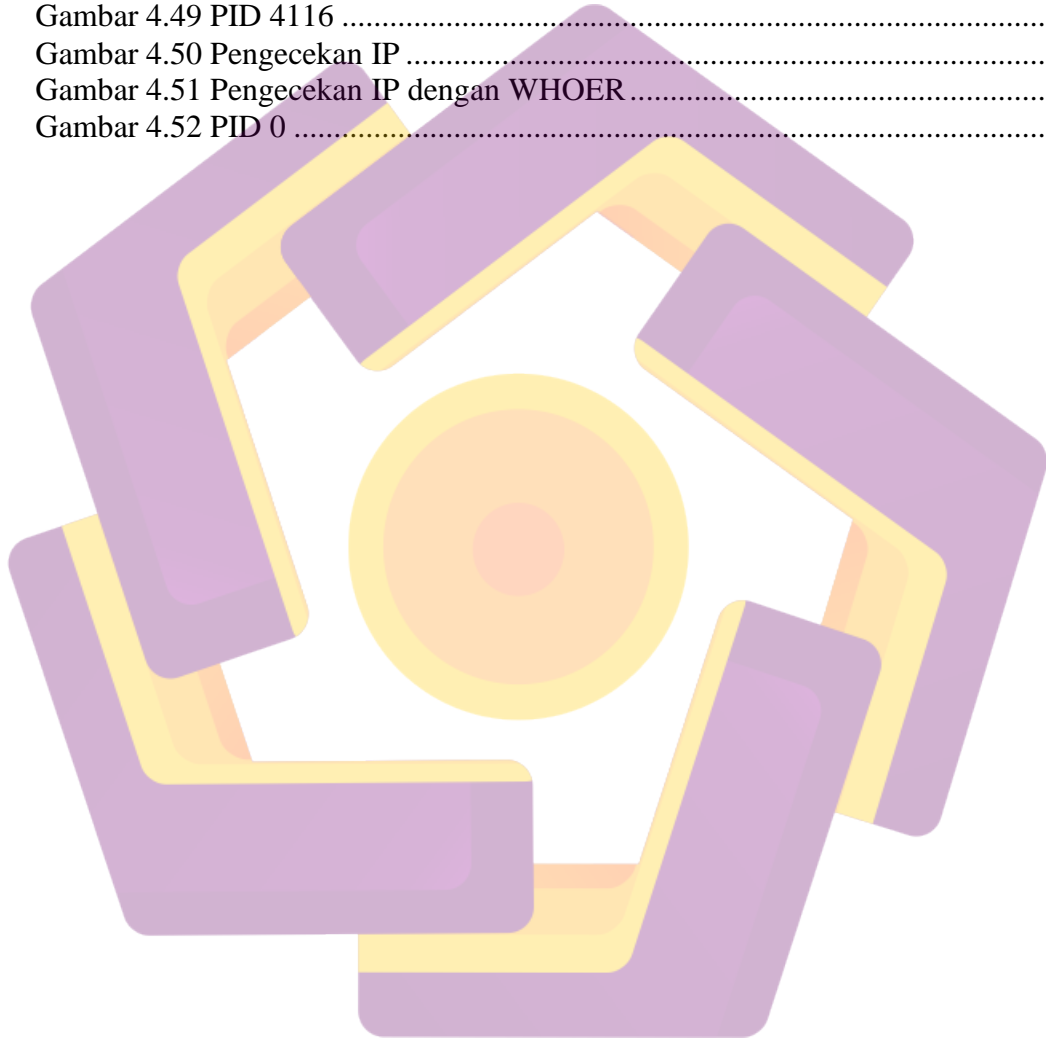
Tabel 2.1 Penelitian Terkait	6
Tabel 3.1 Spesifikasi Hardware	16
Tabel 3.2 Spesifikasi Kali Linux.....	16
Tabel 3.3 Spesifikasi Virtual Enviroment Windows 7.....	17
Tabel 3.4 Tools Pendukung.....	17
Tabel 4.1 Penjelasan Konfigurasi	20
Tabel 4.2 Informasi dasar file malware.....	26
Tabel 4.3 Daftar nama antivirus.....	28
Tabel 4.4 Keterangan dari State.....	31
Tabel 4.5 IP Terkoneksi	44



DAFTAR GAMBAR

Gambar 1.1 Grafik Pendeteksian 20 Malware Macro.....	1
Gambar 3.1 Diagram Alur Penelitian.....	13
Gambar 3.2 Proses Analisis VirusTotal.....	15
Gambar 3.3 Proses Analisis AnyRun.....	15
Gambar 4.1 Msfconsole	19
Gambar 4.2 Penggunaan Module Exploit.....	20
Gambar 4.3 Perintah Konfigurasi Payload.....	20
Gambar 4.4 Pengecekan Konfigurasi.....	21
Gambar 4.5 Pembuatan Malware Menjadi Dokumen Word.....	21
Gambar 4.6 Perintah Pemindahan File Malware	22
Gambar 4.7 Pengeditan file malware	22
Gambar 4.8 Hasil deteksi VirusTotal.....	22
Gambar 4.9 informasi dasar dari malware	23
Gambar 4.10 Antivirus yang menandai sebagai malware.....	24
Gambar 4.11 Antivirus yang menandai sebagai malware.....	25
Gambar 4.12 Antivirus yang menandai sebagai malware.....	25
Gambar 4.13 Skema Jaringan	28
Gambar 4.14 Perintah <i>use exploit/multi/handler</i>	29
Gambar 4.15 Perintah pengaturan payload	29
Gambar 4.16 Pengecekan Konfigurasi.....	29
Gambar 4.17 Perintah untuk memulai serangan	30
Gambar 4.18 Dokumen malware dibuka oleh korban	30
Gambar 4.19 Penyerang terhubung dengan korban	31
Gambar 4.20 Sistem korban telah disusupi Penyerang.....	31
Gambar 4.21 Penyerang Menggunakan Cmd	32
Gambar 4.22 Perintah untuk Menampilkan Daftar File.....	32
Gambar 4.23 Penyerang mematikan komputer korban.....	32
Gambar 4.24 Pendeteksian melalui cmd.....	33
Gambar 4.25 Pengecekan Task Manager.....	35
Gambar 4.26 Pengecekan properties.....	35
Gambar 4.27 Properties Aplikasi	36
Gambar 4.28 Aplikasi Asing.....	36
Gambar 4.29 Penghentian paksa aplikasi yang berjalan	37
Gambar 4.30 Konfirmasi Penghentian Paksa.....	37
Gambar 4.31 Malware telah dimatikan.....	38
Gambar 4.32 Koneksi antara penyerang dan korban telah terputus.....	39
Gambar 4.33 Penghapusan Aplikasi Asing.....	39
Gambar 4.34 Aplikasi asing telah terhapus.....	40
Gambar 4.35 Analisis AnyRun	40
Gambar 4.36 Perintah <i>netstat -n</i>	41
Gambar 4.37 Hasil <i>netstat -n</i>	41
Gambar 4.38 Hasil Analisis AnyRun.....	42
Gambar 4.39 File dan registry telah berubah	42
Gambar 4.40 Informasi hash	43

Gambar 4.41 IP Terhubung.....	44
Gambar 4.42 IP 20.198.162.78	45
Gambar 4.43 PID 5136	45
Gambar 4.44 PID 7308	45
Gambar 4.45 Lokasi Malware.....	46
Gambar 4.46 Hasil Scanning Malware	46
Gambar 4.47 Hasil Scanning Malware	46
Gambar 4.48 Hasil Scanning Malware	46
Gambar 4.49 PID 4116	47
Gambar 4.50 Pengecekan IP	47
Gambar 4.51 Pengecekan IP dengan WHOER.....	48
Gambar 4.52 PID 0	48



INTISARI

Perkembangan *malware* sangat cepat setiap harinya, karena *malware* dapat bersembunyi pada perangkat lunak. Salah satunya adalah perangkat lunak Microsoft Office Word. Perangkat lunak yang satu ini digunakan oleh banyak pengguna. Perangkat lunak yang memiliki banyak fungsi ini, salah satu fungsinya dimanfaatkan penyerang untuk mencuri data. Fungsi yang dimanfaatkan untuk penyerangan pada pengguna Microsoft Office Word adalah fungsi *macro*.

Agar dapat mengetahui bagaimana proses pembuatan *malware* yang memanfaatkan fungsi *macro*, menyerang pengguna, dan mendeteksinya diperlukannya analisis. Analisis dilakukan dengan implementasi pembuatan *malware* menjadi file *doc* yang nantinya dibuka dengan aplikasi Microsoft Office Word oleh korban. *Tool* yang digunakan dalam pembuatan dan penyerangan adalah *Metasploit Framework* pada Linux. Kemudian dilakukan analisis statis pada *malware docm* dengan tool VirusTotal untuk mengetahui informasi yang terdapat pada *malware* serta antivirus yang dapat mengatasinya.

Setelah dilakukannya analisis statis, dilakukannya analisis dinamis dengan penjalanan *malware* untuk mengetahui secara langsung bagaimana aktivitas *malware* tersebut. Selanjutnya dilakukan pendeteksian pada korban dan ditemukan IP penyerang yang terhubung serta aplikasi asing dengan nama asing yang berjalan dilatar belakang.

Kata kunci: *Malware, Macro, Microsoft Office Word, Analisis Statis, Analisis Dinamis*

ABSTRACT

The development of malware is very fast every day, because malware can hide in software. One of them is Microsoft Office Word software. This software is used by many users. This software that has many functions, one of its functions is used by attackers to steal data. The function that is used to attack Microsoft Office Word users is the macro function.

In order to know how the process of creating malware that utilizes macro functions, attacks users, and detects it requires analysis. The analysis is carried out by implementing the malware into a doc file which will be opened by the victim with the Microsoft Office Word application. The tool used in the creation and attack is the Metasploit Framework on Linux. Then a static analysis was carried out on the docm malware with the VirusTotal tool to find out the information contained in the malware and the antivirus that could handle it.

After the static analysis is performed, dynamic analysis is carried out with the running of the malware to find out firsthand how the malware is doing. Next, the victim is detected and found the attacker's IP is connected as well as foreign applications with names running in the background.

Keyword: Malware, Macro, Microsoft Office Word, Static Analysis, Dynamic Analysis

