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

SKRIPSI

Disusun oleh:

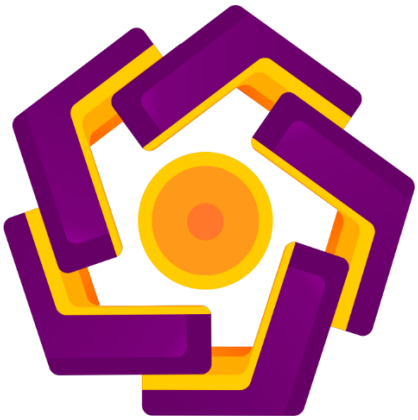
Samuel Sinambela
17.83.0050

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 Sukestyama 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 Al Fatta, M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatatangan 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 Pergururan 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

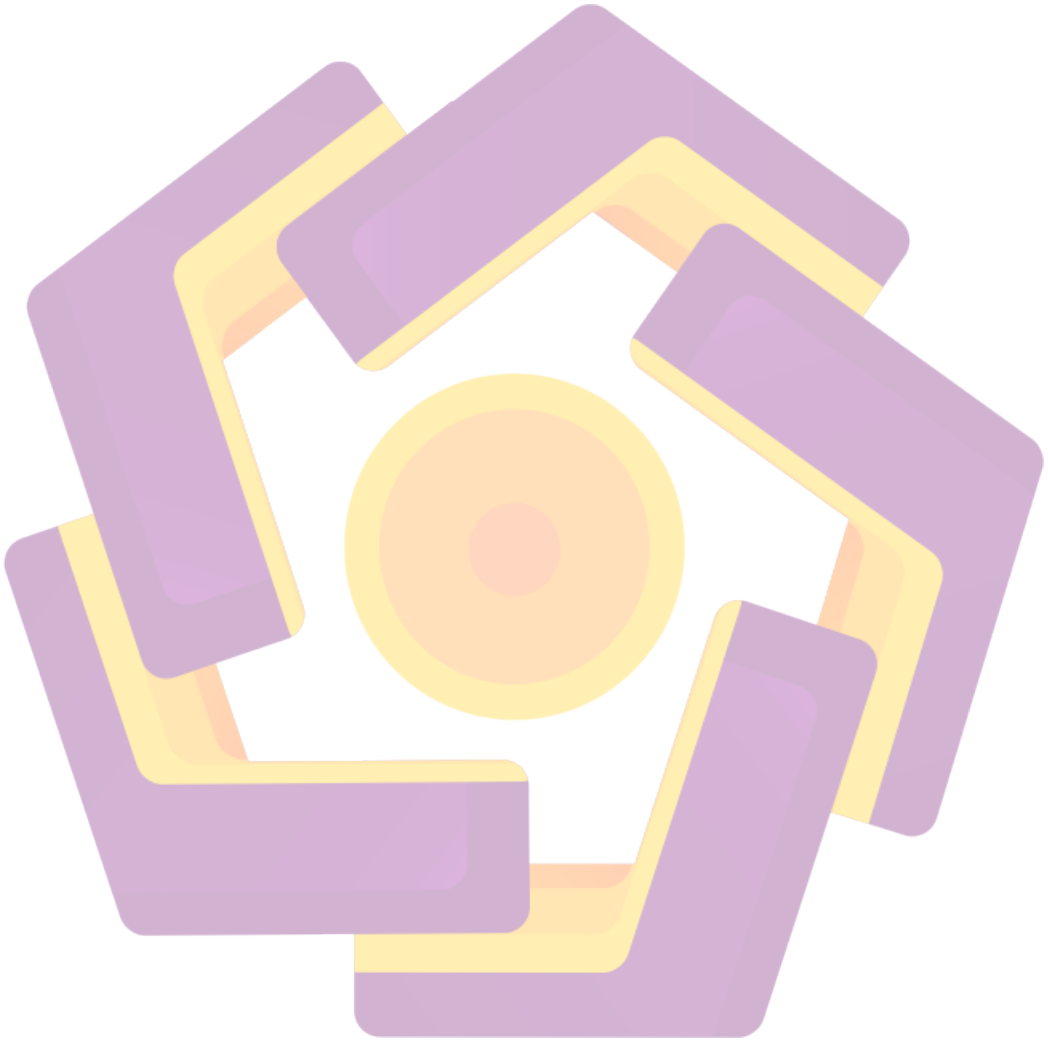
Yang Menyatakan,

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:

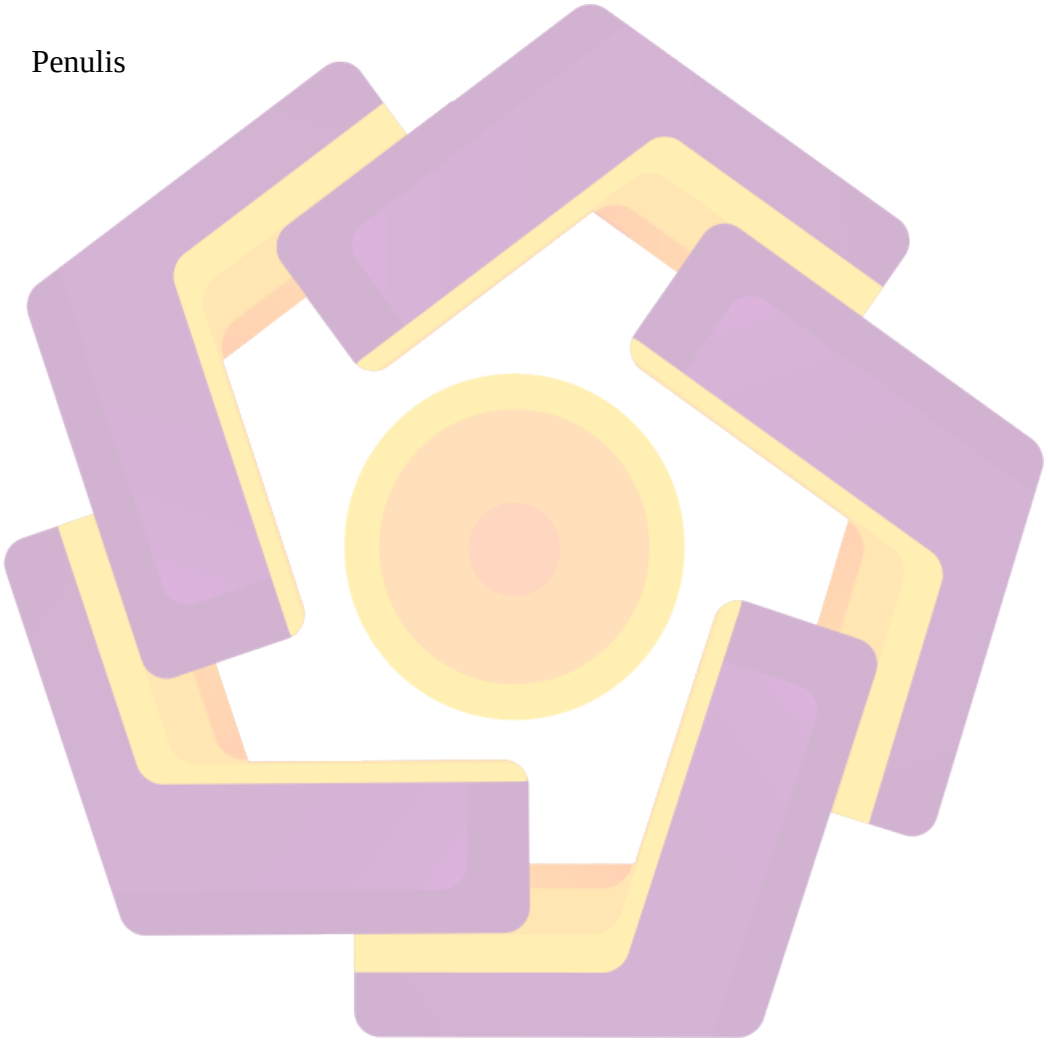
1. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas AMIKOM Yogyakarta.
2. Bapak Dony Ariyus, M. Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta.
3. Bapak Wahyu Sukestyama Putra, S.T., M.Eng. selaku Dosen Pembimbing yang telah bersedia memberikan pengarahan dan 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

DAFTAR TABEL

DAFTAR GAMBAR

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