ANALISIS MALWARE ZOO.APK MENGGUNAKAN METODE ANALISIS STATIS

SKRIPSI

Disusun oleh:

Rafieh Al Abror

17.83.0037

PROGRAM SARJANA

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

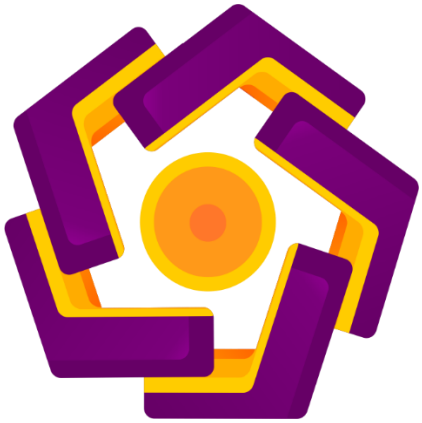
YOGYAKARTA

2022

ANALISIS MALWARE ZOO.APK MENGGUNAKAN METODE ANALISIS STATIS

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:

Rafieh Al Abror

17.83.0037

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS MALWARE ZOO.APK MENGGUNAKAN METODE ANALISIS STATIS

yang dipersiapkan dan disusun oleh

Rafieh Al Abror

17.83.0037

Telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 24 Agustus 2022

Dosen Pembimbing,

Joko Dwi Santoso, M.Kom

NIK. 190302181

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS MALWARE ZOO.APK MENGGUNAKAN METODE ANALISIS STATIS

yang dipersiapkan dan disusun oleh

Rafieh Al Abror

17.833.0037

Telah dipertahankan di depan Dewan Penguji

pada tanggal 24 Agustus 2022

Susunan Dewan Penguji

Nama Penguji	**Tanda Tangan**
Banu Santoso, S.T., M.Eng	
NIK. 190302327	
Senie Destya, M.Kom	
NIK. 190302312	
Joko Dwi Santoso, M.Kom	
NIK. 190302181	

Skripsi ini telah diterima sebagai salah satu persyaratan

untuk memperoleh gelar Sarjana Komputer

Tanggal 20 Agustus 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Rafieh Al Abror
NIM : 17.83.0037

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS *MALWARE ZOO.APK* MENGGUNAKAN METODE ANALISIS STATIS

Dosen Pembimbing : **Joko Dwi Santoso, M.Kom**

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, 24 Agustus 2022

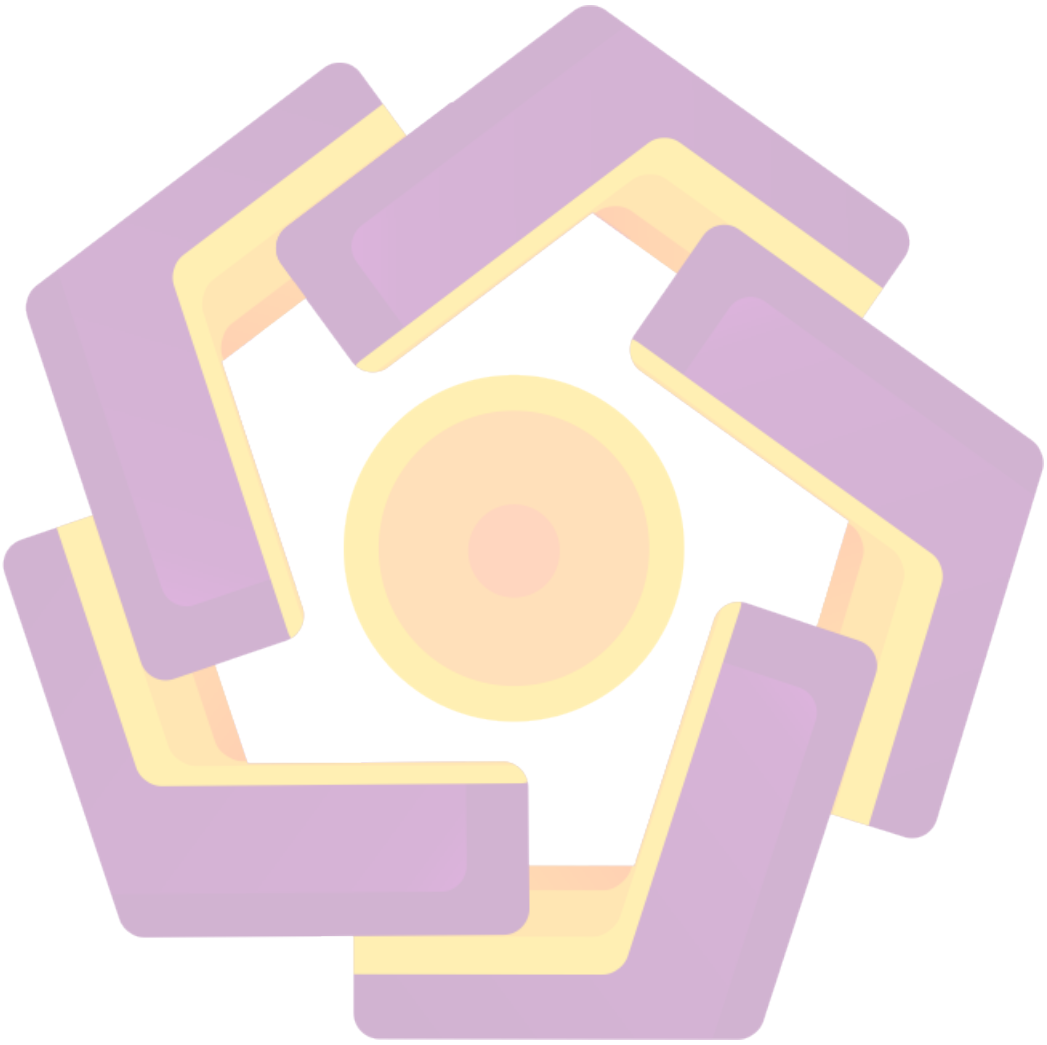
Yang Menyatakan,

Rafieh Al Abror

HALAMAN MOTO

"Sedikit lebih beda, lebih baik daripada sedikit lebih baik"

Seth Godin



HALAMAN PERSEMBAHAN

Dengan segala puji syukur kepada Allah SWT, Tuhan yang Maha Esa dan atas dukungan doa dari orang tua dan orang-orang tercinta, Alhamdulillah skripsi ini dapat diselsaikan . Dengan rasa bahagia dan bangga saya ucapkan rasa syukur dan terimakasih kepada:

1. Allah SWT atas rahmat, anugerah, dan karunianya yang telah diberikan kepada kita semua, sehingga atas ijin Allah SWT lah saya bisa seperti ini.
2. Kedua orang tua, Bapak Dasuki dan Ibu Fitriani yang selalu mendoa'kan, memberi dukungan, fasilitas serta memberikan hasil kerja kerasnya kepada saya.
3. Bapak Bapak Joko Dwi Santoso, M.Kom. selaku dosen pembimbing yang tulus ikhlas membimbing dan mengarahkan serta meluangkan waktunya agar saya menjadi lebih baik lagi.
4. Teman-teman saya yang selalu mengingatkan saya akan mengerjakan skripsi.
6. Seluruh pihak yang tidak dapat saya sebutkan satu per satu, terimakasih atas segala batuan dan do'anya sehingga terselesaikan skripsi ini.

Terimakasih sebesar-besarnya untuk kalian semua, akhir kata saya persembahkan skripsi ini untuk kalian semua, semoga skripsi ini dapat memberikan manfaat yang banyak bagi semua pihak.

KATA PENGANTAR

Puji dan syukur dipanjatkan kehadirat Tuhan Yang Maha Esa atas karunia yang telah dianugerahkan kepada penulis, sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisis *Malware Zoo.Apk* Menggunakan Metode Analisis Statis".

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. Allah SWT karena atas karunia-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan semoga dapat memberikan manfaat di kemudian hari.
2. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas AMIKOM Yogyakarta.
3. Bapak Dony Ariyus, M.Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta.
4. Bapak Joko Dwi Santoro, M.kom. selaku Dosen Pembimbing yang telah bersedia memberikan pengarahan dan bimbingan dalam penyususnan Skripsi ini
5. Segenap Dosen, Staff, dan Karyawan Universitas AMIKOM Yogyakarta yang telah memberikan ilmu kepada penulis di bangku kuliah dan juga membantu penulis dalam kelancaran administrasi sampai terselesaikannya Skripsi ini.
6. Orang tua, saudara-saudara beserta keluarga yang selalu mendoakan dan memberikan dukungan penuh kepada penulis
7. Serta kepada semua pihak yang telah membantu dalam penyusunan Skripsi ini yang tidak dapat penulis sebutkan satu per satu.

Penulis berharap semoga skripsi ini dapat bermamfaat bagi semua pihak yang terkait dalam penulisan ini. Dalam penulisan skripsi ini penulis menyadari masih banyak kekurangan karena terbatasnya pengetahuan dan pengalaman penulis. Karena itu, dengan lapang hati penulis mengharapkan kritik dan saran yang membangun guna menyempurnakan skripsi ini

Yogyakarta, 28 Juli 2022

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Malware atau *malicious software* adalah perangkat lunak yang diciptakan untuk menyusup dan merusak sebuah sistem tanpa persetujuan dari pengguna, seperti *virus, Trojan*, dan lain nya yang dapat disebar melalui jaringan internet. Untuk membuktikan bahwa perangkat lunak tersebut adalah sebuah malware, yaitu dengan cara mengetahui cara kerja dari perangkat lunak tersebut. Dan metode yang digunakan untuk membuktikannya adalah analisis statis yang merupakan metode yang digunakan untuk menganalisa cara kerja dari sebuah perangkat lunak yang dicurigai sebagai *malware.*

Analisis ini dilakukan menggunakan *tool online virustotal* dan *mobile security framework (MobSF)* dengan metode statis pada sampel apk yang dicurigai sebagai *malware.*

Hasil dari analisis *file zoo.apk* yang ditemukan pada *VirusTotal* 30 dari 60 anti-malware mendeteksi *malware* pada *aplikasi zoo.apk*, dan *Framework MobSF* dengan fitur *static analyzer* mendeteksi adanya 4 *permission dangerous* yang ada pada aplikasi *zoo.apk.*

Kata Kunci: Android, APK, Malware, Malware Analysis, Static Analysis

ABSTRACT

Malware or malicious software is software that is created to infiltrate and damage a system without the consent of the user, such as viruses, Trojans, and others that can be spread over the internet. To prove that the software is malware, that is by knowing how the software works. And the method used to prove it is static analysis which is the method used to analyze the workings of a software suspected of being malware.

This analysis was carried out using the virustotal online tool and the mobile security framework (MobSF) with a static method on apk samples suspected of being malware.

The results of the zoo.apk file analysis found in VirusTotal 30 out of 60 anti-malware detected malware in the zoo.apk application, and the MobSF Framework with the static analyzer feature detected 4 dangerous permissions in the zoo.apk application.

Keywords: Android, APK, Malware, Malware Analysis, Static Analysis