ANALISIS MALWARE ANDROID MENGGUNAKAN METODE REVERSE ENGINEERING

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer

disusun oleh

FRENVOL DE SANTONARIO MAGNO MOISES

17.83.0039

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

ANALISIS MALWARE ANDROID MENGGUNAKAN METODE REVERSE ENGINEERING

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

FRENVOL DE SANTONARIO MAGNO MOISES

17.83.0039

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS MALWARE ANDROID MENGGUNAKAN METODE REVERSE ENGINEERING

yang disusun dan diajukan oleh

FRENVOL DE SANTONARIO MAGNO MOISES

17.83.0039

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 27 Februari 2023

Dosen Pembimbing,

Joko Dwi Santoso, M.Kom.
NIK. 190302181

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS MALWARE ANDROID MENGGUNAKAN METODE REVERSE ENGINEERING

yang disusun dan diajukan oleh

FRENVOL DE SANTONARIO MAGNO MOISES
17.83.0039
Telah dipertahankan di depan DeWAN Penguji
pada tanggal 27 Februari 2023

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Joko Dwi Santoso, M.Kom **NIK. 190302181**	
M. Rudyanto Arief, S.T, M.T **NIK. 190302098**	
Melwin Syafrizal, S.Kom., M.Eng. **NIK. 190302105**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 27 Februari 2023

DEKAN FAKULTAS ILMU KOMPUTER

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

HALAMAN PERNYATAAN KEASLIAN *SKRIPSI*

Yang bertandatangan di bawah ini,

Nama mahasiswa : FRENVOL DE SANTONARIO MAGNO MOISES
NIM : 17.83.0039

Menyatakan bahwa *Skripsi* dengan judul berikut:

ANALISIS MALWARE ANDROID MENGGUNAKAN METODE REVERSE ENGINEERING

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, 27 Februari 2023

Yang Menyatakan,

Frenvol De Santonario Magno Moises

iv

HALAMAN PERSEMBAHAN

Segala puji bagi Tuhan Yang Maha Esa atas limpahan rahmat dan hidayah serta karunia-Nya sehingga *skrip*si ini selesai dengan sebaik-baiknya. Skripsi ini saya persembahkan untuk :

1. Kedua orang tua, Bapak Geraldo Moises dan Ibu Durvalina Belo Magno yang selalu mendoa'kan, memberi dukungan, fasilitas serta memberikan hasil kerja kerasnya kepada saya.
2. Bapak Joko Dwi Santoso, M.kom. Selaku dosen pembimbing yang telah membantu dalam penyusunan *skrip*si ini.
3. Kepada kakak serta adik saya yang selalu memberikan semangat dan dukungan.
4. Kepada sahabat dan teman-teman yang ada disaat suka maupun duka selama masa perkuliahan saya.
5. Sesorang yang sangat berharga dan memberikan banyak arti dalam hidup saya, Lidia Kristiani Sihaloho. Terima kasih atas cinta, dukungan, kebaikan, perhatian, dan kebijaksanaan serta telah mengajarkan arti kedewasaan.

Terimakasih yang sebesar-besarnya untuk Kalian semua, akhir kata saya persembahkan skripsi ini untuk Kalian semua, orang-orang yang telah memberikan pengalaman yang sangat berarti dalam hidup saya. Semoga skripsi ini dapat bermanfaat dan berguna untuk kemajuan ilmu pengetahuan di masa yang akan datang.

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* Android Menggunakan Metode *Reverse engineering*".

Skripsi ini disusun sebagai syarat memperoleh gelar Sarjana Komputer pada program Studi S1 Teknik Komputer (S.Kom) 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 :

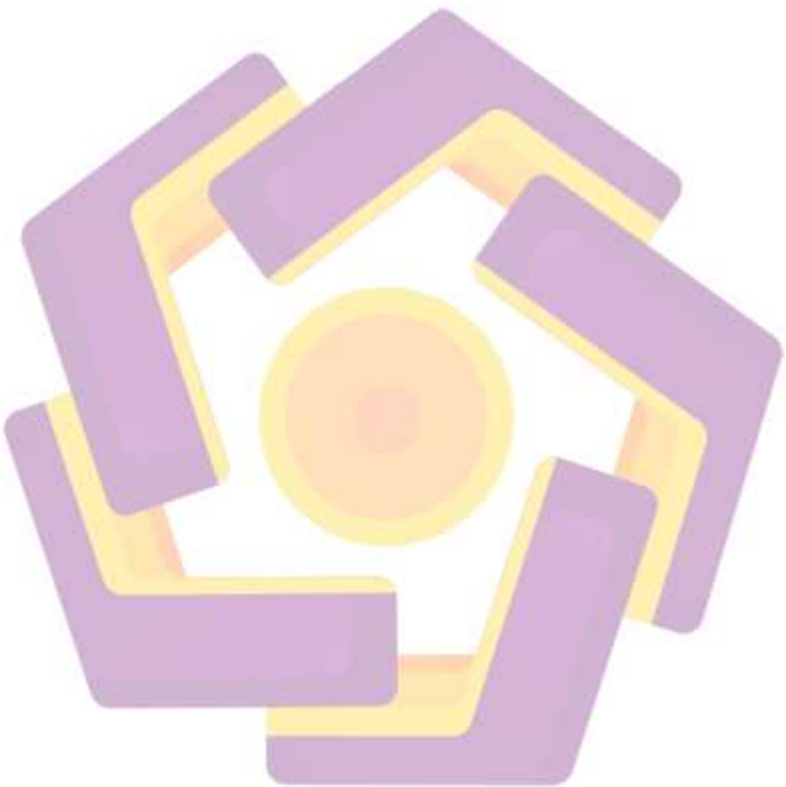
1. Tuhan Yang Maha Esa karena atas karunia-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan semoga dapat memberikan mamfaat di kemudian hari.
2. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas AMIKOM Yogyakarta.
3. Bapak Dony Ariyus, M.Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta.
4. Bapak Joko Dwi Santoso, 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.

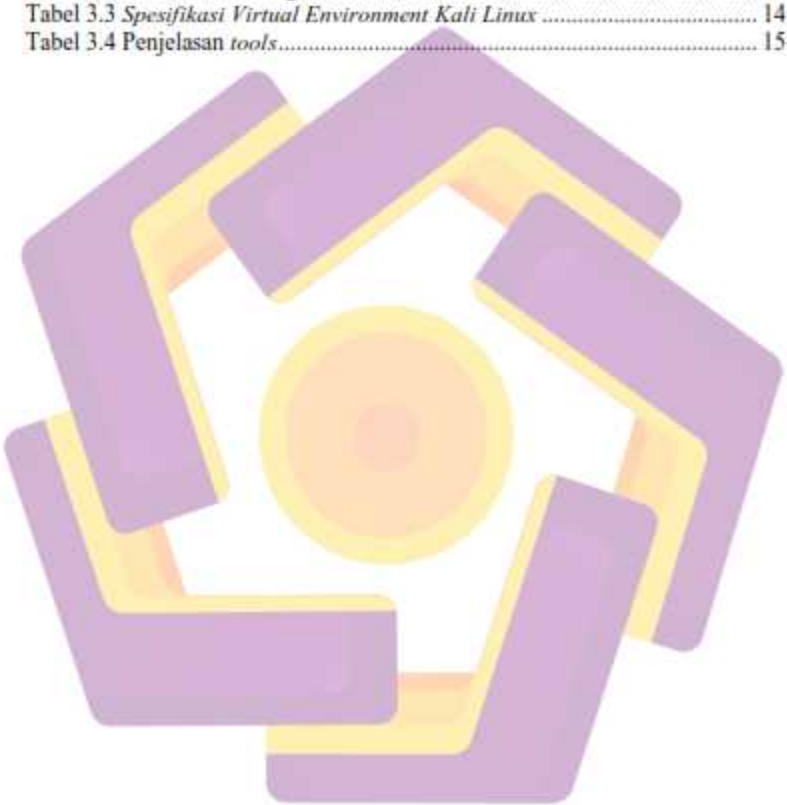
Yogyakarta, 4 Oktober 2022

FRENVOL DE SANTONARIO MAGNO MOISES

DAFTAR ISI



DAFTAR TABEL



DAFTAR GAMBAR

INTISARI

Kemajuan pesat telah dicapai dalam pengembangan teknologi smartphone berbasis Android. Komunikasi, belanja, dan transaksi keuangan hanyalah beberapa dari tugas sehari-hari yang dilakukan orang dengan smartphone mereka. Android, di sisi lain, adalah sistem operasi open-source yang memudahkan siapa saja untuk membuat aplikasi Android yang dapat diakses melalui smartphone. Menghitung aplikasi yang disematkan malware oleh application, salah satunya adalah malware. Analisis dilakukan dengan sample *malware Trojan* pada aplikasi *syssecApp.apk* dengan menggunakan metode *reverse engineering*. dalam melakukan *reverse engineering malware Trojan* menggunakan *tools APKTOOL, JD-GUI*. Penelitian ini akan melakukan analisa terhadap sebauh aplikasi *syssecApp.apk* yang terinfeksi *malware Trojan* dengan menggunakan metode *reverse engineering*. Hasil dari analisis pada aplikasi *syssecApp.apk* ditemukan adanya ip host penerima yang terdapat pada sorce code didalam *syssecApp.apk*

Kata kunci: Android, APK, *Malware*, *Reverse engineering*

ABSTRACT

Rapid progress has been made in the development of Android-based smartphone technology. Communication, shopping and financial transactions are just a few of the daily tasks that people perform with their smartphones. Android, on the other hand, is an open-source operating system that makes it easy for anyone to create Android apps that can be accessed via a smartphone. Counting applications embedded with malware by application, one of which is malware.The analysis was carried out with samples of Trojan malware in the syssecApp.apk application using the reverse engineering method. in doing Trojan malware reverse engineering using APKTOOL tools. JD-GUI.This research will analyze the syssecApp.apk application that infects Trojan malware using the reverse engineering method. The results of the analysis on the syssecApp.apk application found that there is an ip host receiver contained in the source code in syssecApp.apk

Keywords: Android, APK, Malware, Reverse engineering