ANALISIS MALWARE TROJAN MENGGUNAKAN METODE REVERSE ENGINEERING PADA WINDOWS 7

SKRIPSI

Disusun Oleh:

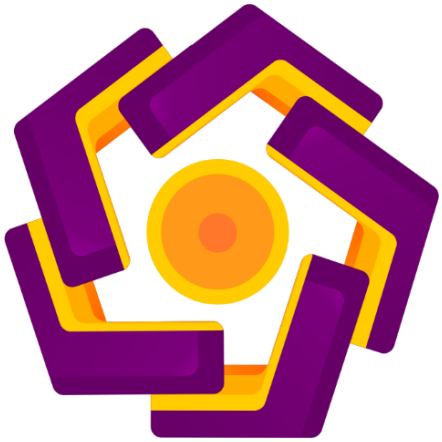
Ade Riyana
17.33.0081

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

ANALISIS MALWARE TROJAN MENGGUNAKAN METODE REVERSE ENGINEERING PADA WINDOWS 7

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:

Ade Riyana
17.83.0081

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

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS MALWARE TROJAN MENGGUNAKAN METODE REVERSE ENGINEERING PADA WINDOWS 7

yang dipersiapkan dan disusun oleh

Ade Riyana
17.83.0081

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 21 Februari 2022

Dosen Pembimbing,

Banu Santoso, S.T., M.Eng
NIK. 190302327

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS MALWARE TROJAN MENGGUNAKAN METODE REVERSE ENGINEERING PADA WINDOWS 7

yang dipersiapkan dan disusun oleh

Ade Riyana
17.83.0081
Telah dipertahankan di depan Dewan Penguji
pada tanggal 21 Februari 2022

Susunan Dewan Penguji

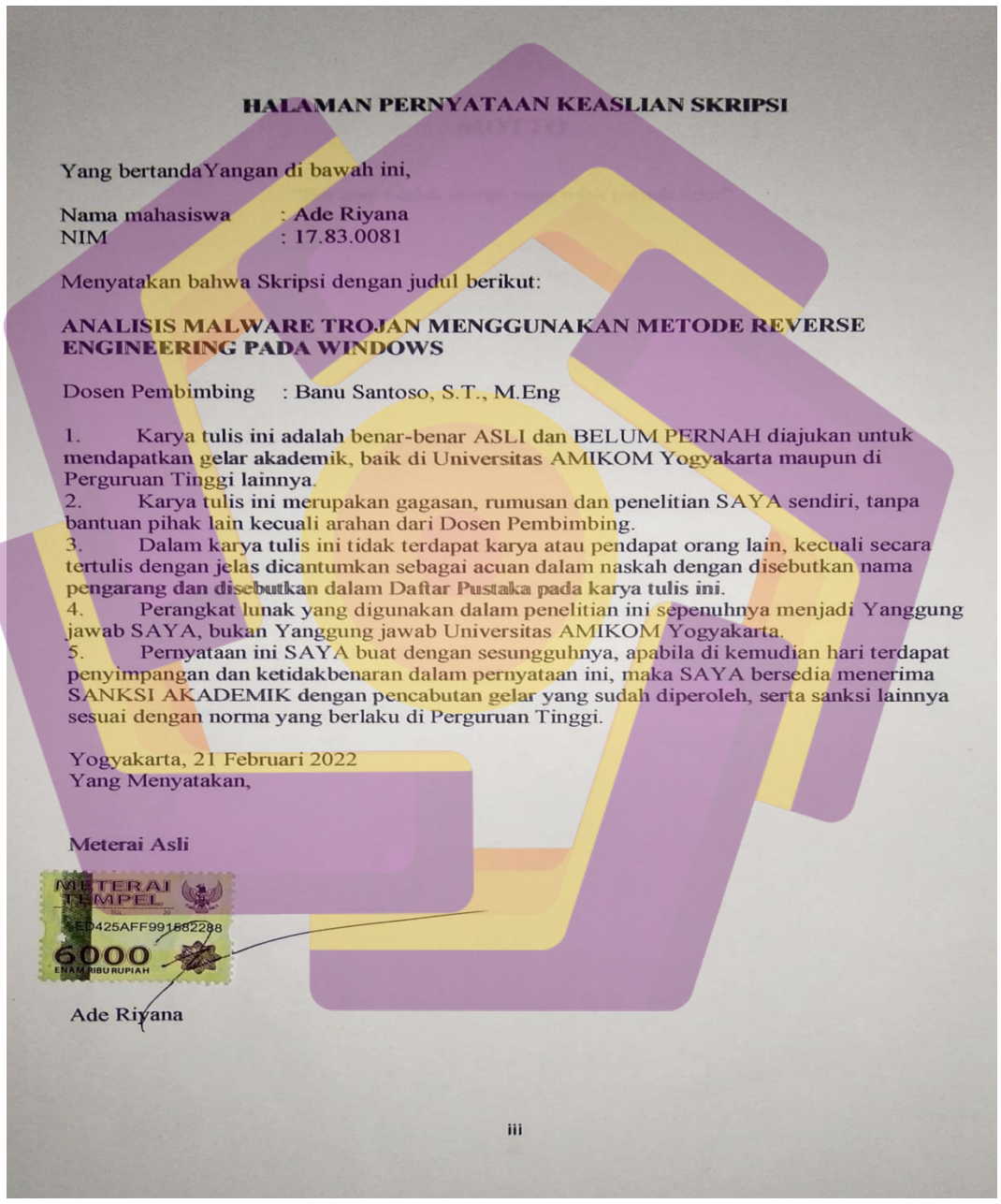
Nama Penguji	Tanda Tangan
Jeki Kuswanto, M.Kom **NIK : 190302456**	
Anggit Ferdita Nugraha, S.T., M.Eng. **NIK : 190302480**	
Banu Santoso, S.T., M.Eng **NIK. 190302327**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 21 Februari 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, S.kom., M.kom.
Nik. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI



HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandaYangan di bawah ini,

Nama mahasiswa : Ade Riyana
NIM : 17.83.0081

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS MALWARE TROJAN MENGGUNAKAN METODE REVERSE ENGINEERING PADA WINDOWS

Dosen Pembimbing : Banu Santoso, 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 Yanggung jawab SAYA, bukan Yanggung 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, 21 Februari 2022
Yang Menyatakan,

Meterai Asli

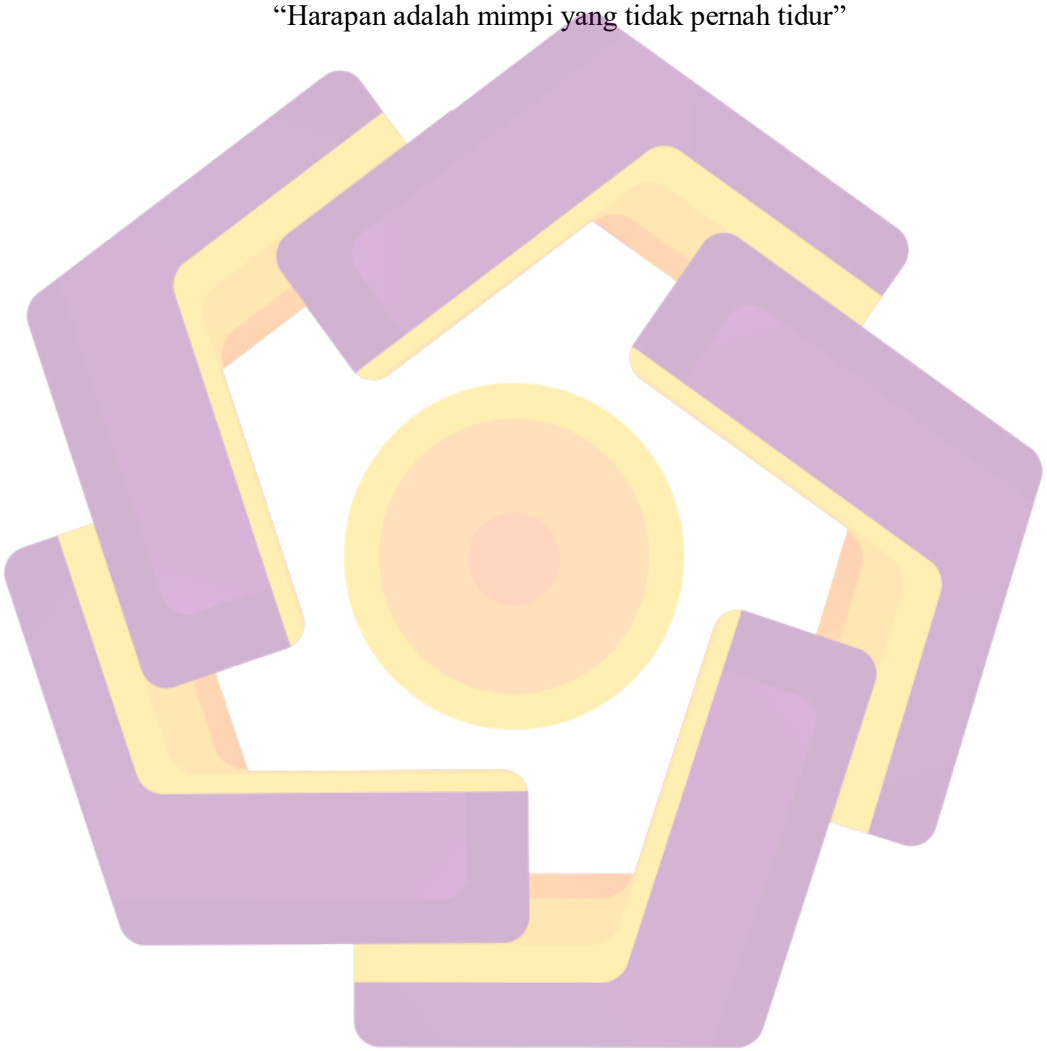
METERAI TEMPEL
ED425AFF991882288
6000
ENAM RIBU RUPIAH

Ade Riyana

iii

MOTTO

“Harapan adalah mimpi yang tidak pernah tidur”



PERSEMBAHAN

Segala puji bagi Allah Subhanahu wa ta'ala, yang senantiasa melimpahkan rahmat-Nya, sehingga penulis dapat menyelesaikan skripsi. Penyusunan skripsi ini tidak lepas dari dukungan dan doa dari orang-orang tercinta sehingga skripsi ini dapat diselesaikan dengan baik. Oleh karena itu, dengan ketulusan hati dan rasa syukur penulis mengucapkan terima kasih kepada:

1. Allah subhanahu wa ta'ala, atas izin dan ridha-Nya Penyusun dapat menyelesaikan skripsi ini dengan baik.
2. Orang tua saya, yang selalu memberikan doa dan banyak dukungan selama kuliah hingga selesai skripsi ini. Semoga Allah subhanahu wa ta'ala senantiasa memberi kebahagiaan dan kemudahan untuk beliau berdua.
3. Dosen pembimbing skripsi, bapak Banu Santoso, S.T., M.Eng, selaku dosen pembimbing yang telah memberi banyak masukan, kritikan, dan saran agar proses pengerjaan dapat selesai dengan baik, serta seluruh dosen di Universitas Amikom Yogyakarta yang telah memberikan banyak ilmu pengetahuan dan pengalaman kepada penulis. Terima kasih atas ilmu serta pengalaman yang telah disampaikan kepada penulis, semoga ilmu yang didapat menjadi berkah dan dapat penulis bagikan kepada orang lain.
4. Rekan – rekan kelas 17 Teknik Komputer 1 dan 2, yang telah memberikan saya dukungan, semangat serta menemani selama perkuliahan dalam satu kelas yang penuh dengan cerita. Terimakasih atas kenangan-kenangan yang telah diukir bersama-sama.

KATA PENGANTAR

Segala puji bagi Allah Subhanahu wa ta'ala, yang senantiasa melimpahkan rahmat-Nya, sehingga penulis dapat menyelesaikan skripsi berupa analisis malware yang berjudul Analisis Malware Trojan Menggunakan Metode Reverse Engineering Pada Windows.

Skripsi yang berupa analisis malware ini sebagai salah satu syarat untuk memenuhi kelulusan di Program S1 Teknik Komputer, Fakultas Ilmu Komputer, Universitas AMIKOM Yogyakarta. Penyusunan skripsi ini tidak terlepas bantuan banyak pihak baik moril maupun materi. penulis ingin mengucapkan terimakasih kepada:

1. Allah subhanahu wa ta'ala yang dengan karunia dan hidayah-Nya penulis dapat menyelesaikan skripsi dengan baik.
2. Prof. Dr. M. Suyanto, MM, selaku Rektor Universitas Amikom Yogyakarta.
3. Ibu Krisnawati, S.Si., M.T. selaku Dekan Fakultas Ilmu Komputer.
4. Bapak Dony Ariyus, M.Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta.
5. Bapak Banu Santoso, S.T., M.Eng, selaku dosen pembimbing yang memberi arahan, dukungan, dan motivasi sehingga penulis dapat menyelesaikan skripsi dengan baik.
6. Bapak dan Ibu dosen S1 Teknik Komputer yang telah memberikan banyak pengalaman dan ilmunya ketika perkuliahan di kelas maupun di laboratorium.
7. Kedua orang tua saya yang telah memberikan banyak semangat dan dukungan hingga skripsi ini selesai.
8. Keluarga besar Teknik Komputer 2017.
9. Semua pihak yang tidak dapat penulis sebutkan satu per satu yang telah membantu dalam proses penyelesaian skripsi ini sehingga skripsi ini dapat terselesaikan.

Terimakasih yang sebesar-besarnya penulis menyadari bahwa penyusunan skripsi ini masih jauh dari sempurna, oleh karena itu penulis mengharapkan kritik dan saran yang membangun untuk penyusunan skripsi yang lebih baik. Akhir kata semoga skripsi ini dapat bermanfaat dan berguna bagi semua yang memerlukannya.

Yogyakarta, 22 Februari 2022

Ade Riyana

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

INTISARI

Incidence response of malware attack atau serangan malware. Penyerangan keamanan sekarang sudah banyak mengalami perkembangan, yang awal nya perorangan (hacker) kini menjadi lebih luas (cyberwar). Tidak menutup kemungkinan untuk seseorang terserang malware pada sistem komputer yang digunakan.. Malware dapat menyerang melalui media offline maupun online seperti sms, chat atau spam (whatsapp, instagram, email, telegram). Banyak yang berpikir bahwa malware dapat dengan mudah diTangani hanya dengan antivirus. Malware memiliki sistem pertahanan sendiri dan dapat menyembunyikan diri dari antivirus atau bahkan menginfeksi antivirus itu. Malware dapat diTangani dengan mengetahui cara kerja ketika melakukan serangan ke dalam sistem komputer.

Analisis malware dilakukan dengan mengimplementasikan malware trojan danabot pada laptop dan komputer menggunakan metode reverse engineering. Aplikasi yang diunduh ternyata trojan yang menyamar, untuk mengetahui apakah benar aplikasi sudah terinfeksi malware perlunya menganalisis terlebih dahulu.

Penelitian ini akan menganalisis aplikasi danabot yang terinfeksi malware trojan dengan metode reverse engineering. Untuk mengecek keaslian malware perlunya mengecek md5 dan sha 256 malware, yang berarti aplikasi danabot yang di download benar telah terinfeksi malware trojan bukan aplikasi yang corrupt atau rusak.

Keyword: *Malware, Trojan DanaBot, Reverse Engineering, Analysis Static, Windows 7.*

ABSTRAK

Incidence response of malware attack or malware attack. Security attacks have now undergone many developments, which were originally individuals (hackers) now becoming more widespread (cyberwars). It is possible for someone to be attacked by malware on the computer system used. Malware can attack through offline or online media such as sms, chat or spam (whatsapp, instagram, email, telegram). Many think that malware can be easily handled with just an antivirus. Malware has its own defense system and can hide itself from an antivirus or even infect it. Malware can be handled by knowing how to work when attacking a computer system.

Malware analysis is carried out by implementing trojan and bot malware on laptops and computers using reverse engineering methods. The downloaded application turns out to be a trojan in disguise, to find out whether the application is indeed infected with malware, it is necessary to analyze it first.

This research will analyze the Danabot application that is infected with trojan malware by reverse engineering method. To check the authenticity of malware, it is necessary to check for md5 and sha256 malware, which means that the downloaded Danabot application has been infected with trojan malware, not a corrupt or damaged application.

***Keyword**: Malware, DanaBot Trojan, Reverse Engineering, Static Analysis, Windows 7.*