ANALISA DAN DETEKSI MALWARE REMOTE ACCESS TROJAN PADA SISTEM OPERASI WINDOWS DAN METODE HYBRID ANALISIS

***SKRIP*SI**

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

MOHAMMAD QHOID

17.83.0019

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

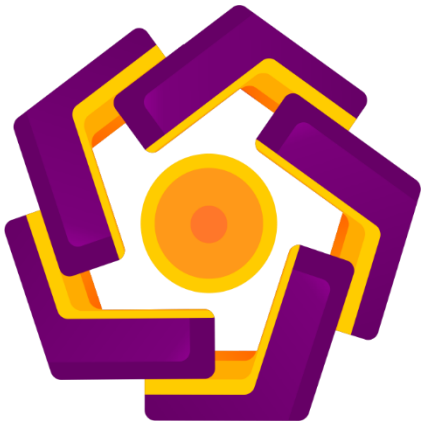
2023

ANALISA DAN DETEKSI MALWARE REMOTE ACCESS TROJAN PADA SISTEM OPERASI WINDOWS DAN METODE HYBRID ANALISIS

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer



disusun oleh

MOHAMMAD QHOID

17.83.0019

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

HALAMAN PERSETUJUAN

SKRIPSI

ANALISA DAN DETEKSI MALWARE REMOTE ACCESS TROJAN PADA SISTEM OPERASI WINDOWS DENGAN METODE HYBRID ANALISIS

yang disusun dan diajukan oleh

MOHAMMAD QHOID

17.83.0019

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 24 JULI 2023

Dosen Pembimbing,

Joko Dwi Santoso, M.Kom.
NIK. 190302181

HALAMAN PENGESAHAN

SKRIPSI

ANALISA DAN DETEKSI MALWARE REMOTE ACCESS TROJAN PADA SISTEM OPERASI WINDOWS DENGAN METODE HYBRID ANALISIS

yang disusun dan diajukan oleh

MOHAMMAD QHOID
17.83.0019
Telah dipertahankan di depan De*WAN* Penguji
pada tanggal 24 JULI 2023

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Joko Dwi Santoso, M.Kom **NIK. 190302181**	
Senie Destya, M.Kom **NIK. 190302312**	
Muhammad Koprawi, S.Kom., M.Eng **NIK. 190302454**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 24 juli 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 : Mohammad Qhoid
NIM : 17.83.0019

Menyatakan bahwa *Skripsi* dengan judul berikut:

ANALISA DAN DETEKSI MALWARE REMOTE ACCESS TROJAN PADA SISTEM OPERASI WINDOWS DAN METODE HYBRID ANALISIS

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 JULI 2023

Yang Menyatakan,

MOHAMMAD QHOID

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 purnomo dan ibu marfuah yang selalu mendoakan, 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 keluarga besar Drs.KH.abdurrahman yang telah memberikan semangat dan dukungan, baik secara material atau secara visual.
5. Semua pihak yang mendukung saya secara langsung ataupun tidak langsung.

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 "Analisa Dan Deteksi Malware Remote Access Trojan Pada Sistem Operasi Windows Dan Metode Hybrid Analisis".

*Skrip*si 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. Allah SWT karena atas karunia-nya,sehingga penulis dapat menyelesaikan skripsi dengan baik dan semoga dapat memberikan barokah 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, 24 juli 2023

Mohammad Qhoid

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Perkembangan masa adalah jenis - jenis malware yang muncul di dunia maya semakin beragam. Trojan adalah salah satu jenis malware yang ikut berkembang di dalamnya, yang memungkinkan attacker masuk ke dalam sistem tanpa diketahui oleh pemilik. Penggunaan trojan saat ini lebih ke arah kejahatan dunia maya (cyber crime). Cara kerja trojan yang cepat dan handal menjadi penyebab penggunaan trojan semakin marak dalam dunia kejahatan komputer. Sasaran terbanyak penyebaran trojan adalah pengguna sistem operasi Windows. memungkinkan penyebaran trojan ini dilakukan dengan metode social-engineering, teknik yang menggunakan kelemahan manusia, sehingga user tanpa curiga langsung mengeksekusi sebuah.

Malware analysis adalah metode untuk mengetahui keberadaan malware (malicious software) dalam suatu executable file yang dibagi dalam dua buah tahap yaitu static analysis dan dynamic analysis. Static analysis dilakukan tanpa menjalankan malware tersebut ke dalam sistem seperti disassembly dan debugging, sedangkan dynamic analysis dilakukan dengan menjalankan malware dalam sistem untuk melihat process detail, file system activity, registry activities, dan network traffic. Dengan menggabungkan hasil dari static malware analysis dan dynamic malware analysis diperoleh karakteristik malware yang dijadikan data rekomendasi untuk mendeteksi keberadaan trojan malware pada executable file Windows.

Kata kunci: Trojan, social engineering, malware analysis, executable file

ABSTRACT

The development of the times is the types of malware that appear in cyberspace are increasingly diverse. Trojan is one type of malware that is also developing in it, which allows attackers to enter the system without being noticed by the owner. The current use of trojans is more towards cybercrime. The fast and reliable way of working trojans is the reason why the use of trojans is increasingly widespread in the world of computer crime. The most common target for trojans is users of the Windows operating system. allows the spread of this trojan is done by the method of social-engineering, a technique that uses human weaknesses, so that the user without suspecting a direct execute a.

Malware analysis is a method to determine the presence of malware (malicious software) in an executable file which is divided into two stages, namely static analysis and dynamic analysis. Static analysis is done without running the malware into the system such as disassembly and debugging, while dynamic analysis is done by running malware in the system to view process details, file system activity, registry activities, and network traffic. By combining the results of static malware analysis and dynamic malware analysis, malware characteristics are obtained which are used as recommendation data to detect the presence of trojan malware in Windows executable files.

Keywords: Trojans, social engineering, malware analysis, executable files