# ANALISIS MALWARE TROJAN DOWNLOADER MENGGUNAKAN METODE REVERSE ENGINEERING

**SKRIPSI**


Disusun oleh:

**Ipung Ardiansyah**

**17.83.0107**


**PROGRAM SARJANA**

**PROGRAM STUDI TEKNIK KOMPUTER**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS AMIKOM YOGYAKARTA**

**YOGYAKARTA**

**2021**

# ANALISIS MALWARE TROJAN DOWNLOADER MENGGUNAKAN METODE REVERSE ENGINEERING

## 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:

**Ipung Ardiansyah**

**17.83.0107**


**PROGRAM SARJANA**
**PROGRAM STUDI TEKNIK KOMPUTER**
**FAKULTAS ILMU KOMPUTER**
**UNIVERSITAS AMIKOM YOGYAKARTA**
**YOGYAKARTA**
**2021**

## HALAMAN PERSETUJUAN

## SKRIPSI

**ANALISIS MALWARE TROJAN DOWNLOADER MENGGUNAKAN METODE REVERSE ENGINEERING**

yang dipersiapkan dan disusun oleh

**Ipung Ardiansyah**

**17.83.0107**

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 18 Desember 2020

**Dosen Pembimbing,**

**Joko Dwi Santoso, M.Kom**

**NIK. 190302181**

# HALAMAN PENGESAHAN

## SKRIPSI

### ANALISIS MALWARE TROJAN DOWNLOADER MENGGUNAKAN METODE REVERSE ENGINEERING

yang dipersiapkan dan disusun oleh

**Ipung Ardiansyah**

**17.83.0107**

Telah dipertahankan di depan Dewan Penguji
pada tanggal 15 Januari 2021

**Susunan Dewan Penguji**

| Nama Penguji | Tanda Tangan |
|---|---|
| **(Joko Dwi Santoso, M.Kom)**<br>**NIK. 190302181** | |
| **(Sudarmawan, S.T., M.T.)**<br>**NIK. 190302035** | |
| **(Hendra Kurniawan, M.Kom)**<br>**NIK. 190302244** | |

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 15 Januari 2021

**DEKAN FAKULTAS ILMU KOMPUTER**

**Krisnawati, S.Si, M.T.**
**NIK. 190302038**

## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini.
**Nama mahasiswa : Ipung Ardianoyah**
**NIM : 17.83.0107**

Menyatakan bahwa Skripsi dengan judul berikut:

**Analisis Malware Trojan Downloader 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, 15 Januari 2021
Yang Menyatakan,

Ipung Ardianoyah



v

## HALAMAN MOTTO

"Dream It, Believe It, Then Build It."

"Sebuah Langkah Kecil Merupakan Sebuah Awal Yang Begitu Panjang"
(Gus Baha)

## HALAMAN PERSEMBAHAN

Dengan segala puji dan syukur kepada Tuhan yang Maha Esa dan atas dukungan dan doa dari orang-orang tercinta, akhirnya skripsi ini dapat diselesaikan dengan baik. Oleh karena itu, dengan rasa bangga dan bahagia saya khaturkan rasa syukur dan terimakasih saya kepada :

1. Allah SWT, Tuhan Yang Maha Esa karena hanya atas izin dan karunia-Nyalah, maka skripsi ini dapat dibuat dan selesai pada waktunya. Puji syukur yang tak terhingga pada Tuhan semesta alam yang meridhoi dan mengabulkan segala doa.
2. Orang tua saya, yang tidak pernah lelah memberikan saya dukungan dan doa. Untuk Ibu yang tidak pernah lelah dalam memberikan semangat supaya saya bisa menyelesaikan skripsi ini dan untuk Bapak yang telah banyak memberikan begitu banyak pengorbanan yang tidak bisa saya balaskan. Terimakasih banyak saya ucapkan untuk keduanya.
3. Dosen Pembimbing skripsi bapak Joko Dwi Santoso, M.Kom. selaku dosen pembimbing saya, saya sangat berterimakasih atas bimbingannya selama ini yang telah memberikan masukan, kritik dan saran yang membangun agar menjadi lebih baik lagi untuk kedepannya. serta seluruh jajaran dosen Universitas Amikom Yogyakarta yang sudah membagikan ilmunya saya mengucapkan terimakasih, semoga ilmu dari bapak dan ibu dosen bisa saya amalkan ke yang lain juga.
4. Rekan – rekan kelas 17 Teknik Komputer 2, yang telah memberikan saya dukungan, semangat serta menemani selama 3 tahun dalam satu kelas yang penuh dengan segala kondisi dalam hidup. Terimakasih atas kenangan-kenangan yang telah kita ukir bersama-sama. Semoga kita menjadi orang-orang yang bermanfaat dan dikenang menjadi pribadi yang baik.
5. Keluarga besar Himpunan Teknik Komputer, Keluarga besar Senat Mahasiswa dan Keluarga Besar PMII Amikom Yogyakarta, yang telah

mendidik saya dan memberikan pengalaman yang begitu banyak dalam segala aspek.

6. Keluarga besar Omah Jogja, Keluarga besar Softex Camp, serta Keluarga besar Pondok Pesantren Madrasah Hidayatul Mubtadiin (MHM) Saung Dadi, yang telah memberikan dukungan, semangat serta keceriaan selama saya bersama rekan-rekan semua.

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

*Assalamualaikum Warahmatullahi Wabarakatuh*

Puji syukur penulis panjatkan kehadirat Allah SWT yang selalu melimpahkan rahmat serta hidayah-Nya kepada setiap hamba-Nya. Skripsi ini disusun sebagai salah satu syarat kelulusan Program Strata 1 Program Studi Teknik Komputer, Universitas AMIKOM Yogyakarta dan untuk memperoleh gelar Sarjana Komputer (S.Kom).

Dengan selesainya skripsi yang berjudul ***"Analisis Malware Trojan Downloader Menggunakan Metode Reverse Engineering"***, dengan ini penyusun ingin mengucapkan terima kasih kepada :.

1. Allah SWT atas rahmat, hidayah, serta karunia-Nya yang telah diberikan kepada penulis sehingga skripsi ini dapat terselesaikan.
2. Prof. Dr. M. Suyanto, MM selaku rektor Universitas AMIKOM Yogyakarta
3. Ibu Krisnawati, S.Si., M.T. selaku Dekan Fakultas Ilmu Komputer dan Ketua Program Studi S1 Sistem Informasi.
4. Bapak Dony Ariyus, M.Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas AMIKOM Yogyakarta
5. Kedua orang tua, yang selalu memberikan dukungan baik materi maupun doa.
6. Bapak Joko Dwi Santoso, M.Kom. selaku dosen pembimbing yang tidak bosan memberikan arahan, saran dan motivasi agar penulis bisa mengerjakan naskah ini dengan baik dan benar.
7. Bapak dan Ibu Universitas AMIKOM Yogyakarta yang telah memberikan ilmunya selama penulis kuliah.
8. Keluarga besar kelas S1 Teknik Komputer 02 angkatan 2017.
9. Keluarga besar Himpunan Teknik Komputer angkatan 2017 – 2019.

10. Keluarga besar Senat Mahasiswa angkatan 2019 – 2020.
11. Keluarga besar PMII Amikom Yogyakarta.
12. Keluarga besar Omah Jogja dan Softex Camp.
13. Keluarga besar Pondok Pesantren Madrasah Hidayatul Mubtadiin (MHM) Saung Dadi.
14. Serta semua pihak yang telah membantu dalam proses penyusunan skripsi ini yang tidak dapat disebutkan satu per satu.

Akhirnya dengan kerendahan hati penulis mengucapkan terimakasih dan semoga skripsi ini dapat bermanfaat bagi penulis maupun pembaca.

*Wassalamualaikum Warahmatullahi Wabarakatuh*

Yogyakarta, 15 Januari 2021

Penulis

**DAFTAR ISI**

## DAFTAR TABEL

## DAFTAR GAMBAR

## INTISARI

Perkembangan teknologi ponsel cerdas berplatfrom *android* telah mencapai kemajuan yang sangat pesat. Ponsel cerdas membantu dan memudahkan pekerjaan manusia sehari – hari seperti berkomunikasi, berbelanja, hingga transaksi keuangan. Namun karena *android* merupakan sistem *open-source*, siapapun dapat dengan mudah mengembangkan aplikasi *android* yang dapat diunduh di *android app market*. Termasuk aplikasi yang disisipkan *malware* oleh pengembang aplikasi, salah satunya adalah *malware trojan downloader*.

Analisis dilakukan dengan mengimplementasikan penginfeksiaan *malware trojan downloader* pada aplikasi kamus kesehatan menggunakan metode *reverse engineering*. Penginfeksiaan *malware trojan downloader* menggunakan *tools metasploit framework*. Aplikasi akan terinfeksi *payload* yang diciptakan dari *metasploit framework*.

Penelitian ini akan melakukan analisa terhadap aplikasi kamus kesehatan sebelum dan sesudah terinfeksi *malware trojan downloader* dengan menggunakan metode *reverse engineering*. Hasil dari analisis pada aplikasi kamus kesehatan ditemukan perbedaan ukuran aplikasi menjadi 10.17 MB yang sebelumnya adalah 10.05 MB. Tentunya dengan perubahan ukuran file, maka secara otomatis juga perubahan pada *hashing SHA256*. Pada bagian *permissions*, ditemukan perbedaan yang sebelumnya hanya ada 9 *permissions*, namun setelah terinfeksi ditemukan 18 *permissions* tambahan sehingga total keseluruhan menjadi 27 *permissions*.



**Kata kunci:** *Malware, Trojan Downloader, Reverse Engineering, Android*

## *ABSTRACT*

*The development of smartphone technology with the Android platform has made very rapid progress. Smartphones help and facilitate daily human work such as communicating, shopping, and financial transactions. However, because android is an open-source system, anyone can easily develop android applications that can be downloaded on the android app market. Including applications that have been inserted by malware by application developers, one of which is the Trojan downloader malware.*

*The analysis was carried out by implementing the Trojan downloader malware infection in the health dictionary application using the reverse engineering method. Trojan downloader malware infection uses metasploit framework tools. The application will be infected with the payload created from the metasploit framework.*

*This study will analyze the health dictionary application before and after being infected with the Trojan downloader malware using the reverse engineering method. The results of the analysis on the health dictionary application found that the difference in the size of the application was 10.17 MB, which previously was 10.05 MB. Of course, by changing the file size, the SHA256 hashing changes automatically. In the permissions section, it was found that there were only 9 permissions before being infected, but after being infected, we found 18 additional permissions, bringing the total to 27 permissions.*



**Keyword:** *Malware, Trojan Downloader, Reverse Engineering, Android*