

**ANALISIS MALWARE TROJAN DOWNLOADER
MENGUNAKAN 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
MENGUNAKAN 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
MENGUNAKAN 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
MENGUNAKAN 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)
NIK. 190302181



(Sudarmawan, S.T., M.T.)
NIK. 190302035



(Hendra Kurniawan, M.Kom)
NIK. 190302244



Skrripsi 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 Ardianayah

NIM : 17.53.0107

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:



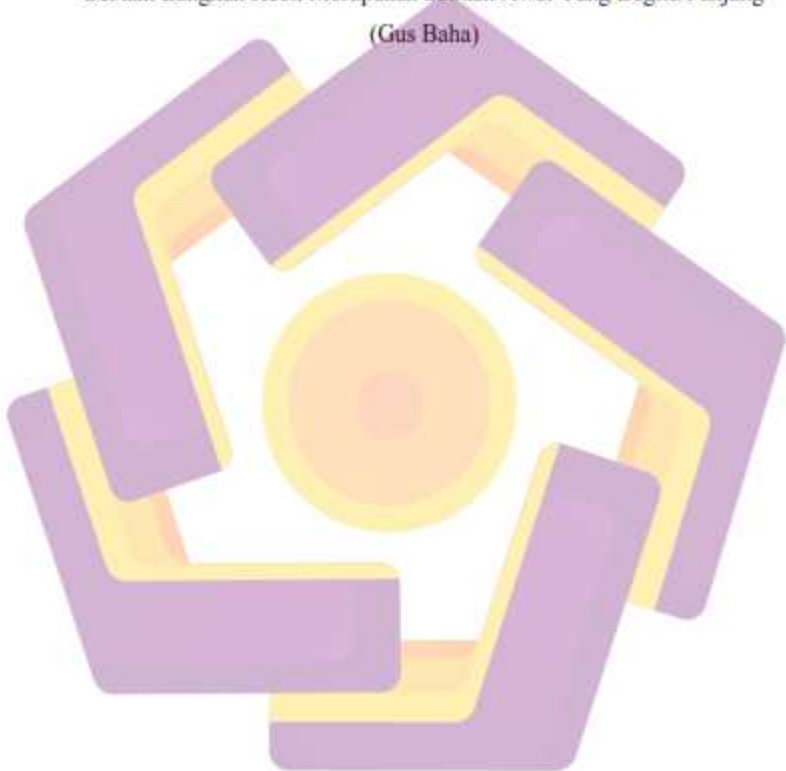
Ipung Ardianayah

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 kehadiran 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

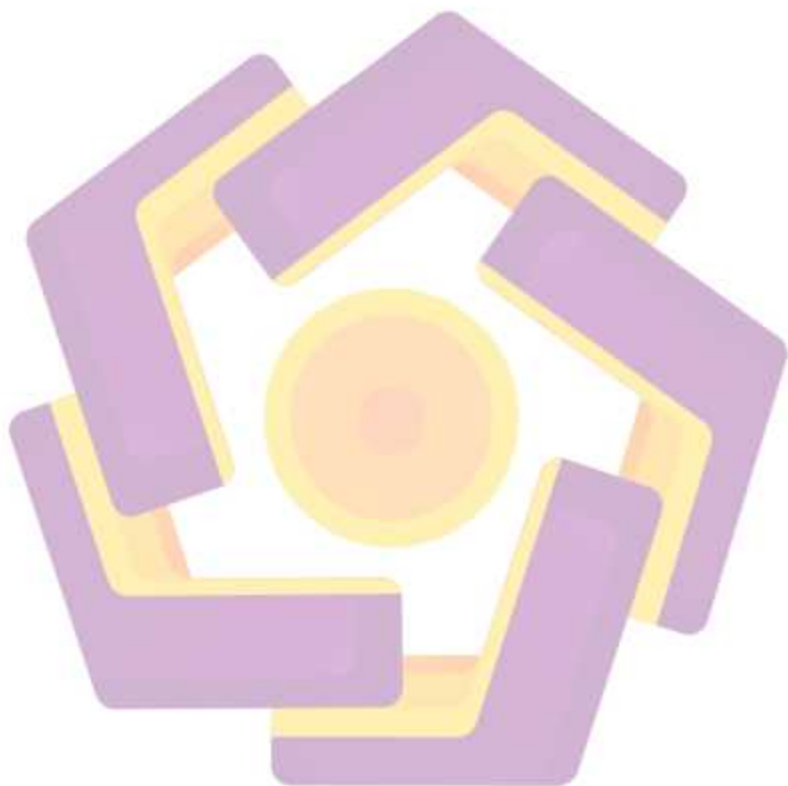
DAFTAR ISI

HALAMAN JUDUL.....	2
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....	v
HALAMAN MOTTO.....	vi
HALAMAN PERSEMBAHAN.....	vii
KATA PENGANTAR.....	ix
DAFTAR ISI.....	xi
DAFTAR TABEL.....	xv
DAFTAR GAMBAR.....	xvi
INTISARI.....	xix
<i>ABSTRACT</i>	xx
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian.....	4
1.5 Sistematika Penulisan.....	5
BAB II LANDASAN TEORI	6
2.1 Tinjauan Pustaka.....	6
2.2 Malware.....	14
2.3 Klasifikasi Malware.....	14
2.3.1 Contagious Threats (Ancaman yang menular).....	14
2.3.2 Masked Threats (Ancaman bertopeng).....	15
2.3.3 Financial Threats (Ancaman keuangan).....	16
2.4 Trojan Downloader.....	16
2.5 Analisis Malware.....	17
2.5.1 Analisis Statis.....	17

2.5.2 Analisis Dinamis.....	19
2.5.3 Analisis Hybrid.....	19
2.6 Reverse Engineering.....	19
2.6.1 Assembly.....	20
2.6.2 Disassembly.....	20
2.6.3 Debugging.....	20
2.6.4 x86 Architecture.....	20
2.6.5 Instruction.....	21
2.6.6 Hashing.....	21
2.6.7 String Analysis.....	21
2.6.8 MAER (Malware Analysis Environment and Requirement).....	21
2.6.9 Repository Malware.....	21
2.7 Android.....	21
2.8 Arsitektur Android.....	22
2.9 Metasploit Framework.....	25
2.10 Mobile Security Framework (MobSF).....	25
2.11 Genymotion.....	25
2.12 MARA Framework.....	25
2.13 JD-GUI.....	26
2.14 Payload.....	26
2.15 Exploit.....	27
BAB III METODOLOGI PENELITIAN.....	28
3.1 Gambaran Umum Penelitian.....	28
3.2 Malware dan Aplikasi yang dianalisis.....	28
3.3 Solusi yang diusulkan.....	28
3.4 Alat dan Bahan Penelitian.....	29
3.3.1 Perangkat Keras (<i>Hardware</i>).....	29
3.3.2 Perangkat Lunak (<i>Software</i>).....	30

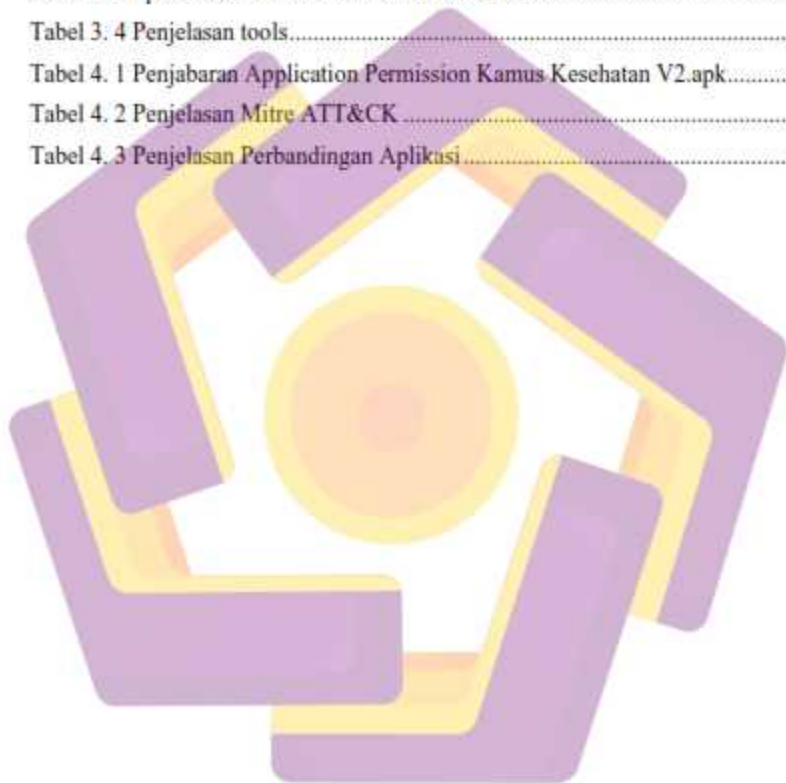
3.5	Metode Penelitian	31
3.5.1	Pre-Experimental Design.....	31
3.5.2	One Group Pretest Posttest Design.....	31
3.5.3	Pengumpulan Data.....	32
3.5.4	Perancangan dan Simulasi.....	32
3.5.5	Dokumentasi.....	32
3.5.6	Flowchart Penelitian.....	32
BAB IV PEMBAHASAN.....		34
4.1	Rancangan Sistem.....	34
4.1.1	Instalasi Virtual Machine Enviroment.....	34
4.1.2	Setting Network.....	35
4.1.3	Instalasi Tools.....	37
4.2	Implementasi Sistem.....	45
4.2.1	Embedded Malware Trojan	45
4.2.2	Malware testing: Checksum Sample Malware.....	47
4.2.3	Decompiler Aplikasi.....	49
4.2.4	Application Permission Analysis	51
4.2.5	Analisis Source Code	55
4.2.6	Metrik Mitre ATT&CK.....	59
4.3	Pengujian Sistem.....	65
4.3.1	Demonstrasi Add Virtual Devices pada Genymotion	65
4.3.2	Demostrasi Setting Network pada Device Genymotion.....	68
4.3.3	Demonstrasi Attack Devices	71
4.3.4	Demonstrasi Perbandingan Aplikasi Sebelum dan Sesudah terdampak Malware Trojan.....	78
BAB V PENUTUP.....		84

5.1 Kesimpulan	84
5.2 Saran	86
DAFTAR PUSTAKA	87



DAFTAR TABEL

Tabel 2. 1 Penelitian yang terkait.....	8
Tabel 3. 1 Daftar Solusi	28
Tabel 3. 2 Spesifikasi Perangkat Keras (Hardware)	29
Tabel 3. 3 Spesifikasi Virtual Enviroment Kali Linux	30
Tabel 3. 4 Penjelasan tools.....	30
Tabel 4. 1 Penjabaran Application Permission Kamus Kesehatan V2.apk.....	52
Tabel 4. 2 Penjelasan Mitre ATT&CK	60
Tabel 4. 3 Penjelasan Perbandingan Aplikasi.....	82



DAFTAR GAMBAR

Gambar 1. 1 Data pengguna ponsel cerdas di dunia	1
Gambar 1. 2 Data serangan mobile aplikasi Q3 2020.....	2
Gambar 1. 3 Data Serangan Trojan Downloader pada Q3 2020.....	3
Gambar 2. 1 Pembagian kelas malware	14
Gambar 2. 2 Representasi Hierarchal berbagai teknik deteksi Malware	17
Gambar 2. 3 Arsitektur Android	23
Gambar 3. 1 Rumus One Groups Pretest-Posttest Design	31
Gambar 3. 2 Flowchart Penelitian.....	33
Gambar 4. 1 Import File OVA Kali-linux-2020.1-vbox-amd64	35
Gambar 4. 2 Proses Impor File OVA di VirtualBox.....	35
Gambar 4. 3 Bridged Adapter Virtual Enviroment Kali Linux	36
Gambar 4. 4 Konfigurasi Network Kali linux.....	37
Gambar 4. 5 Konfigurasi Name Resolver.....	37
Gambar 4. 6 Instalasi MSFVenom.....	38
Gambar 4. 7 Inisiasi Git Clone pada tools MARA Framework.....	38
Gambar 4. 8 Direktori MARA Framework.....	38
Gambar 4. 9 Dashboard MARA Framework.....	39
Gambar 4. 10 Inisiasi perintah Git Clone pada tools jd-gui.....	39
Gambar 4. 11 Instalasi JD-GUI.....	40
Gambar 4. 12 Bahasa Instalasi Genymotion.....	40
Gambar 4. 13 Select Destination Location Genymotion	41
Gambar 4. 14 Select Start Menu Folder Genymotion.....	41
Gambar 4. 15 Select Additional Tasks Genymotion.....	42
Gambar 4. 16 Install Genymotion.....	42
Gambar 4. 17 Proses Instalasi Genymotion	43
Gambar 4. 18 Tampilan Genymotion.....	43
Gambar 4. 19 Metasploit Framework	44
Gambar 4. 20 Inisiasi Git clone MobSF	44
Gambar 4. 21 Masuk ke direktori MobSF	45

Gambar 4. 22 Menjalankan MobSF	45
Gambar 4. 23 Dashboard MobSF.....	45
Gambar 4. 24 Embedded malware trojan pada aplikasi Kamus Kesehatan.....	46
Gambar 4. 25 File Output Aplikasi yang di-embedded	47
Gambar 4. 26 Aplikasi terdeteksi Android Trojan Downloader	47
Gambar 4. 27 Checksum aplikasi kamus kesehatan V2.apk.....	48
Gambar 4. 28 Visualisasi grafik gaya malware pada aplikasi	49
Gambar 4. 29 Proses Decompiler Kamus Kesehatan V2.apk.....	50
Gambar 4. 30 Hasil decompiler Kamus Kesehatan V2.apk.....	51
Gambar 4. 31 Application Permission Kamus Kesehatan V2.apk.....	52
Gambar 4. 32 Decompiler file java menggunakan jd-gui.....	55
Gambar 4. 33 Class yang dieurigai	56
Gambar 4. 34 Analisis file a.class.....	57
Gambar 4. 35 Analisis file e.class.....	57
Gambar 4. 36 Analisis file Tamdj.class	58
Gambar 4. 37 Analisis file lejxi.class	58
Gambar 4. 38 Analisis wakeLock Mxedd.class.....	58
Gambar 4. 39 Analisis socket Mxedd.class	59
Gambar 4. 40 Pemetaan TTP dengan menggunakan Mitre ATT&CK.....	60
Gambar 4. 41 Add Virtual Devices.....	65
Gambar 4. 42 Devices Samsung Galaxy S10.....	65
Gambar 4. 43 Pengaturan Name, Display, dan System pada Devices.....	66
Gambar 4. 44 Pengaturan Android system options dan Network mode.....	66
Gambar 4. 45 Prose Instalasi Devices.....	66
Gambar 4. 46 Start Device	67
Gambar 4. 47 Starting virtual device	67
Gambar 4. 48 Homepage Device	68
Gambar 4. 49 Icon Wifi	68
Gambar 4. 50 Pengaturan SSID AndroidWiFi.....	69
Gambar 4. 51 Network Details AndroidWiFi.....	69
Gambar 4. 52 IP Setting Device.....	70

Gambar 4. 53 Starting Metasploit.....	71
Gambar 4. 54 Exploit Multi Handler	71
Gambar 4. 55 Set Payload.....	71
Gambar 4. 56 Set LHOST.....	72
Gambar 4. 57 Set LPORT	72
Gambar 4. 58 Exploit Device.....	72
Gambar 4. 59 Berhasil Remote Device.....	72
Gambar 4. 60 Dashboard Aplikasi Kamus Kesehatan v2.....	73
Gambar 4. 61 Berhasil melakukan Eksploitasi.....	73
Gambar 4. 62 Command Sysinfo.....	73
Gambar 4. 63 Command ifconfig	74
Gambar 4. 64 Command app_list	74
Gambar 4. 65 Command play	75
Gambar 4. 66 Command screenshot	75
Gambar 4. 67 Hasil dari screenshot devices korban	75
Gambar 4. 68 Command dump_callog	76
Gambar 4. 69 Hasil dari dump call log	76
Gambar 4. 70 Command dump_sms.....	76
Gambar 4. 71 Hasil dari dump sms.....	77
Gambar 4. 72 Command Send Sms	77
Gambar 4. 73 Hasil dari send sms ke perangkat korban.....	78
Gambar 4. 74 Perbandingan tahapan Hashing	78
Gambar 4. 75 Perbandingan tahapan Permissions Sebelum Diinstal	79
Gambar 4. 76 Perbandingan Tahapan Permissions Setelah Diinstal	79
Gambar 4. 77 Perbandingan tahapan Signer Certificate	80
Gambar 4. 78 Perbandingan tahapan Services	81
Gambar 4. 79 Perbandingan tahapan Receivers.....	81

INTISARI

Perkembangan teknologi ponsel cerdas berplatform *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 penginfeksiaian *malware trojan downloader* pada aplikasi kamus kesehatan menggunakan metode *reverse engineering*. Penginfeksiaian *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*