

HALAMAN PERNYATAAN ORISINALITAS

Tugas Akhir / Proyek Akhir / Skripsi / Tesis / Desertasi Ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Eko Putro try Harianto

NPM : 16360501

Tanggal : 3 Juli 2019



HALAMAN PERNYATAAN NON PLAGIAT

Saya yang bertanda tangan di bawah ini :

Nama : Eko Putro Try Harianto

NPM : 16360501

Mahasiswa : Teknik Informatika

Tahun Akademik : 2018/2019

Menyatakan bahwa saya tidak melakukan kegiatan plagiat dalam penulisan Tugas Akhir yang berjudul UJI MALWARE YANG TERIDENTIFIKASI RENTAN TERHADAP WINDOWS KEDALAM ANDROID MENGGUNAKAN METODE REVERSE ENGINEERING.

Apabila suatu saat nanti terbukti melakukan plagiat, maka saya menerima sanksi yang telah ditetapkan.

Demikian Surat Pernyataan ini saya buat dengan sebenar-benarnya.

Jakarta,



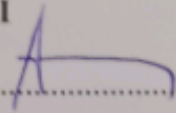
Eko Putro Try Harianto

HALAMAN PENGESAHAN

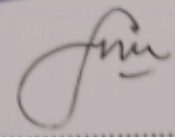
Skripsi ini diajukan oleh :
Nama : Eko Putro Try Harianto
NPM : 16360501
Program Studi : Teknik Informatika
Judul Proyek Akhir : UJI MALWARE YANG TERIDENTIFIKASI
RENTAN TERHADAP WINDOWS
KEDALAM ANDROID MENGGUNAKAN
METODE REVERSE ENGINEERING

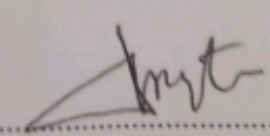
Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh Sarjana Komputer pada Program Studi Teknik Informatika, Fakultas Sains dan Teknologi Informasi, Institut Sains Dan Teknologi Nasional

DEWAN PENGUJI

Pembimbing : Ir. Andi Suprianto, M.Kom (..........)

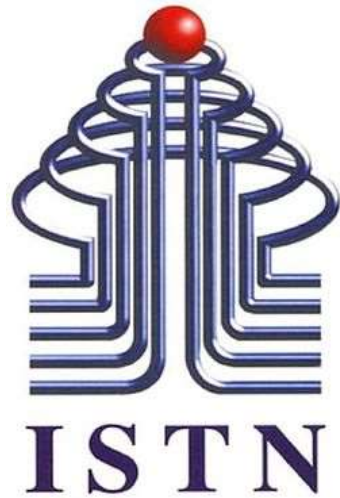
Penguji : Dudy Fadly S., ST, MT (..........)

Penguji : Siti Madinah L., S.Kom, M.Kom (..........)

Penguji : Aryo Nur Utomo, ST, M.Kom (..........)

Ditetapkan di : Jakarta

Tanggal : 3 Juli 2019



**UJI MALWARE YANG TERIDENTIFIKASI RENTAN
TERHADAP WINDOWS KEDALAM ANDROID
MENGUNAKAN METODE REVERSE ENGINEERING**

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar S.Kom

Eko Putro Try Harianto

NIM 16360501

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI INFORMASI

INSTITUT SAINS DAN TEKNOLOGI NASIONAL

JAKARTA

Juli 2019

HALAMAN PERNYATAAN ORISINALITAS

Tugas Akhir / Proyek Akhir / Skripsi / Tesis / Desertasi Ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Eko Putro try Harianto

NPM : 16360501

Tanggal : 3 Juli 2019

HALAMAN PERNYATAAN NON PLAGIAT

Saya yang bertanda tangan di bawah ini :

Nama : Eko Putro Try Harianto

NPM : 16360501

Mahasiswa : Teknik Informatika

Tahun Akademik : 2018/2019

Menyatakan bahwa saya tidak melakukan kegiatan plagiat dalam penulisan Tugas Akhir yang berjudul UJI MALWARE YANG TERIDENTIFIKASI RENTAN TERHADAP WINDOWS KEDALAM ANDROID MENGGUNAKAN METODE REVERSE ENGINEERING.

Apabila suatu saat nanti terbukti melakukan plagiat, maka saya menerima sanksi yang telah ditetapkan.

Demikian Surat Pernyataan ini saya buat dengan sebenar-benarnya.

Jakarta,

Eko Putro Try Harianto

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh :

Nama : Eko Putro Try Harianto

NPM : 16360501

Program Studi : Teknik Informatika

Judul Proyek Akhir : UJI MALWARE YANG TERIDENTIFIKASI
RENTAN TERHADAP WINDOWS
KEDALAM ANDROID MENGGUNAKAN
METODE REVERSE ENGINEERING

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh Sarjana Komputer pada Program Studi Teknik Informatika, Fakultas Sains dan Teknologi Informasi, Institut Sains Dan Teknologi Nasional

DEWAN PENGUJI

Pembimbing : Ir. Andi Suprianto, M.Kom (.....)

Penguji : Dudy Fadly S., ST, MT (.....)

Penguji : Siti Madinah L., S.Kom, M.Kom (.....)

Penguji : Aryo Nur Utomo, ST, M.Kom (.....)

Ditetapkan di : Jakarta

Tanggal : 3 Juli 2019

KATA PENGANTAR

Puji syukur saya panjatkan kehadiran Allah SWT Yang Maha Pengasih dan Maha Penyayang, karena atas berkat rahmat dan karuniaNya, saya tidak dapat menyelesaikan skripsi ini. Penulisan skripsi ini dilaksanakan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Program Studi Teknik Informatika pada Fakultas Sains Dan Teknologi Informasi Institut Sains dan Teknologi Nasional. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak dari masa perkuliahan sampai penyusunan skripsi ini, sangatlah sulit bagi saya untuk menyelesaikan skripsi ini. Oleh karena itu, saya mengucapkan terimakasih kepada :

1. Ir. Andi Suprianto, M.kom, selaku dosen pembimbing Tugas Akhir saya yang telah menyediakan waktunya untuk membimbing saya;
2. Pusat Studi Forensika Digital Universitas Islam Indonesia yang telah membantu dalam mengarahkan dan memberikan berbagai data yang saya butuhkan dalam penyusunan tugas akhir ini;
3. Segenap Tim komunitas *Malware Researcher, Indonesia HoneyNet Project* yang telah membantu dalam memberikan masukan terkait judul dan penulisan skripsi ini;
4. Orang Tua dan Keluarga yang banyak berkorban material dan moral kepada saya; dan
5. Sahabat yang telah banyak membantu saya dalam menyelesaikan skripsi ini

Akhir kata, saya berharap Allah SWT akan membalas segala kebaikan semua pihak yang telah membantu. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu pengetahuan.

Jakarta, 3 Juli 2019

Penulis

Eko Putro Try Harianto

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika Institut Sains Dan Teknologi Nasional, saya yang bertanda tangan di bawah ini :

Nama : Eko Putro Try Harianto

NPM : 16360501

Fakultas : Fakultas Sains Dan Teknologi Informasi

Jenis Karya : Proyek Akhir/ Skripsi/ Tesis/ Disertasi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Institut Sains dan Teknologi Nasional **Hak Bebas Royalti Noneksklusif** (*Non-exclusive Royalty- Free Right*) atas karya ilmiah saya yang berjudul :

UJI MALWARE YANG TERIDENTIFIKASI RENTAN TERHADAP
WINDOWS KEDALAM ANDROID MENGGUNAKAN METODE
REVERSE ENGINEERING

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Institut Sains dan Teknologi Nasional berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*) *soft copy* dan *hard copy*, merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada Tanggal : 3 Juli 2019

Yang menyatakan

Eko Putro Try harianto

ABSTRAK

Nama : Eko Putro Try Harianto

Program Studi : Teknik Informatika

Judul : UJI MALWARE YANG TERIDENTIFIKASI RENTAN
TERHADAP WINDOWS KEDALAM ANDROID
MENGUNAKAN METODE REVERSE ENGINEERING

Malware merupakan salah satu masalah yang cukup serius dalam dunia Teknologi Informasi dan Komunikasi. *Malware* adalah program yang dibuat dalam tujuan khusus untuk mencari sebuah kerentanan pada sebuah sistem. Dalam perkembangannya ada beberapa metode dalam melakukan investigasi dan analisa sampel *malware* diantaranya adalah analisa dinamis, analisa statis, dan *reverse engineering*. Metode *Reverse Engineering* yaitu melakukan proses pembongkaran sampel dimana sampel tersebut akan ditemukan lengkap dengan *source code*, *injection code*, dan *Library* dalam melakukan aksi injeksinya. Terdapat beberapa *tools* dalam melakukan pendeteksian, investigasi, dan pengujian pada sampel diantaranya adalah *cuckoo sandbox*, *Ida Pro*, *MASM*.

Kata kunci : *Malware*, *Reverse Engineering*, *source code*, *injection code*, *Library*, *cuckoo sandbox*, *Ida Pro*, *MASM*.

ABSTRACT

Name : Eko Putro Try Harianto
Study Program : Information Technology
Title : VARIETY IDENTIFIED TEST MALWARE
TOWARDS ANDROID IN WINDOWS USING
REVERSE ENGINEERING METHODS

Malware is one of the serious problems in the world of Information and Communication Technology. Malware is a program created in a special purpose to find a vulnerability in a system. In its development there are several methods in conducting investigations and analysis of malware samples including dynamic analysis, static analysis, and reverse engineering. The Reverse Engineering method is to conduct a sample disassembly process where the sample will be found complete with source code, injection code, and library in carrying out the injection action. There are several tools for detecting, investigating, and testing the sample including cuckoo sandbox, Ida Pro, MASM.

Kata kunci : *Malware, Reverse Engineering, source code, injection code, Library, cuckoo sandbox, Ida Pro, MASM.*

DAFTAR ISI

JUDUL	i
PERNYATAAN ORISINALITAS	ii
PERNYATAAN NON PLAGIAT	iii
PENGESAHAN	iv
KATA PENGANTAR	v
PERYATAAN PERSETUJUAN PUBLIKASI	
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS	vi
ABSTRAK	vii
ABSTRACT	viii
DAFTAR ISI.....	ix
DAFTAR GAMBAR	xiii
DAFTAR TABEL.....	xvii
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	4
BAB 2 TINJAUAN PUSTAKA	5
2.1 Pengertian Sistem Operasi	5

2.1.1	Arsitektur Sistem Operasi Windows.....	5
2.1.2	Arsitektur Sistem Operasi Android.....	9
2.2	Pengertian Komputer Virus	13
2.2.1	Worm	13
2.2.2	Malware.....	14
2.2.3	Spyware.....	14
2.2.4	Ransomware.....	14
2.2.5	Adware	15
2.3	Pemetaan Malware.....	16
2.4	Analisa malware	16
2.4.1	Analisa Statis.....	16
2.4.2	Analisa Dinamis.....	16
2.4.2.1	Runtime Analysis.....	16
2.4.2.2	Surface Analysis.....	16
2.4.3	Reverse Engineering	17
2.4.3.1	Assembly	17
2.4.3.2	Disassembly	17
2.4.3.3	Debugging.....	18
2.4.3.4	X86 Arsitektur	18
2.4.3.5	Instruction	18
2.4.3.6	Hashing	18
2.4.3.7	String Analysis	19
2.4.3.8	MAER (Malware Analysis Environment and Requirement).....	19

2.4.3.9 Repository Malware	19
2.5 Teknologi Sandbox	19
BAB 3 METODOLOGI PENELITIAN.....	21
3.1 Metode Pengumpulan Data	21
3.1.1 Studi Pustaka.....	21
3.1.2 Observasi.....	21
3.1.3 Wawancara	21
3.2 Metode Perangkat Lunak	32
3.3 Bahan Penelitian.....	32
3.4 Tempat dan Waktu Penelitian	32
3.5 Prinsip Penelitian	32
BAB 4 IMPLEMENTASI.....	35
4.1 Define Malware.....	35
4.2 Goal Malware Analysis.....	36
4.3 MAER (Malware Analysis Environment and Requirements)	36
4.4 Dynamic Analysis	42
4.5 Convert to Assembly and Debugging	51
4.6 Convert to Java.....	55
4.7 Use to Android	55
4.8 Pengujian.....	64
4.8.1 Tipe Malware	66
4.8.2 Target Penyerangan.....	66
4.8.2.1 Android 4.4	67
4.8.2.2 Android 5.5	67

4.9 Perbedaan Sistem Operasi Sebelum dan Susudah Terinfeksi Malware	67
4.9.1 Windows	68
4.9.2 Android	68
4.10 Pencegahan.....	69
BAB 5 PENUTUP	71
5.1 Kesimpulan	71
5.2 Saran.....	72
DAFTAR PUSTAKA	73

DAFTAR GAMBAR

Gambar 2.1	Arsitektur Windows	6
Gambar 2.2	Arsitektur Android	10
Gambar 2.3	Peta Serangan Siber	15
Gambar 3.1	SoP Metode Reverse Engineering	22
Gambar 3.2	Define Malware	23
Gambar 3.3	Dynamic Analysis	24
Gambar 3.4	Convert to Assembly, Debugging	25
Gambar 3.5	Convert to Java	26
Gambar 3.6	Alur Tahap Perbaikan Kode.....	27
Gambar 3.7	Alur Tahap Penyisipan Backdoor	27
Gambar 3.8	Diagram Alur Analisa Malware Reverse Engineering	29
Gambar 3.9	Alur Penelitian	32
Gambar 4.1	Hasil Scanning Sampel	35
Gambar 4.2	Vmware 10	36
Gambar 4.3	Guest Windows Xp	37
Gambar 4.4	Guest Windows 7	37
Gambar 4.5	Guest Linux Ubuntu Server 14.04 Lts	38
Gambar 4.6	Guest Linux Kali 2018.03	38

Gambar 4.7	Guest Android 1.1	39
Gambar 4.8	Guest Android 4.4	39
Gambar 4.9	Guest Android 7.1	40
Gambar 4.10	Guest Android 14.1	40
Gambar 4.11	Guest Android 5.5	41
Gambar 4.12	Netbeans IDE 8.0	42
Gambar 4.13	Gambar 4.13 guest Windows7 didalam guest Ubuntu server 14.04 Cuckoo Sandbox	43
Gambar 4.14	Perintah pemanggilan cuckoo guest pada terminal Ubuntu server 14.04 Cuckoo Sandbox	43
Gambar 4.15	Perintah pemanggilan cuckoo host pada terminal Ubuntu server 14.04 Cuckoo Sandbox	44
Gambar 4.16	Upload file pada cuckoo sandbox	44
Gambar 4.17	Proses Analisa cuckoo sandbox	45
Gambar 4.18	Pilihan analysis pada cuckoo sandbox	45
Gambar 4.19	Summary atau ringkasan analysis dari cuckoo sandbox	46
Gambar 4.20	Static Analysis cuckoo sandbox	46
Gambar 4.21	String dari sampel yang ditulis pada cuckoo sandbox	47
Gambar 4.22	Registry yang disusupi oleh sampel	47
Gambar 4.23	Registry yang disusupi oleh sampel.....	48
Gambar 4.24	Network Analysis pada cuckoo sandbox	48
Gambar 4.25	Dropped Buffers	49
Gambar 4.26	Image Memory Guest yang sudah terinfeksi	49
Gambar 4.27	Agent Cuckoo Sandbox pada Guest Windows7	50

Gambar 4.28	File-file Dari sampel	50
Gambar 4.29	File-file Dari sampel	51
Gambar 4.30	Tampilan awal Ida Pro atau Ida Debugging.....	52
Gambar 4.31	Upload sampel sebelum diproses pencarian kode assembly	52
Gambar 4.32	Debug file dan pemecahan kode Hexa dan menjadi Assembly	53
Gambar 4.33	Proses Pencarian String pada kode Hexa	53
Gambar 4.34	Pemecahan kode Hexa menjadi Assembly	54
Gambar 4.35	Pemecahan Kode Hexa menjadi Assembly Menggunakan String Analysis	54
Gambar 4.36	Masuk kedalam tools DosBox dan menjalankan command prompt dan direktori pada windows DOS	56
Gambar 4.37	Proses compile pada MASM	56
Gambar 4.38	Proses Perbaikan Kode Injeksi Java	57
Gambar 4.39	Kode Injeksi dijadikan file.jar	58
Gambar 4.40	Membongkar File Aplikasi android di linux Kali 2018.3	58
Gambar 4.41	Isi File Aplikasi android di kali linux yang akan disisipi file backdoor	59
Gambar 4.42	Isi file aplikasi android yang asli diubah menjadi file file kode injeksi	60
Gambar 4.43	Compile project dan kode injeksi menjadi file apk	60
Gambar 4.44	Sistem Operasi Target Android 4.4 Lenovo A1000.....	61
Gambar 4.45	Download file backdoor	61
Gambar 4.46	Instal file backdoor	62
Gambar 4.47	File backdoor sudah terinstal	62

Gambar 4.48 File mengeksekusi dan membuat program dan hp pada posisi freeze	62
Gambar 4.49 Download file backdoor	63
Gambar 4.50 Eksekusi file backdoor pada terminal emulator	63
Gambar 4.51 Gambar diagram black box testing.....	65
Gambar 4.52 Windows 7 yang belum terinfeksi	68
Gambar 4.53 Windows 7 telah terinfeksi	68
Gambar 4.54 Windows 7 telah terinfeksi	68
Gambar 4.55 OS Android Normal	69
Gambar 4.56 OS Android Normal	69
Gambar 4.57 Android Mati Karena Hardware yang terserang malware	69
Gambar 4.58 Update Patch	70
Gambar 4.59 Install dan Update Antivirus	70
Gambar 4.60 Scan URL dan File	70

DAFTAR TABEL

Tabel 4.1	Pengujian Black Box Malware	66
Tabel 4.2	Pengujian Black Box Target Sistem Operasi Android	66