TUGAS AKHIR

ANALISIS *MALWARE* PADA *EVIL-DROID* MENGGUNAKAN APLIKASI TELEGRAM DENGAN METODE *REVERSE ENGINEERING*

NADYA SADIRA VERDAYANI

20102276

PROGRAM STUDI S1 TEKNIK INFORMATIKA
FAKULTAS INFORMATIKA
INSTITUT TEKNOLOGI TELKOM PURWOKERTO
2024

TUGAS AKHIR

ANALISIS *MALWARE* PADA *EVIL-DROID* MENGGUNAKAN APLIKASI TELEGRAM DENGAN METODE *REVERSE ENGINEERING*

MALWARE ANALYSIS ON EVIL-DROID USING TELEGRAM APPLICATION WITH REVERSE ENGINEERING METHOD

Disusun Sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Komputer

NADYA SADIRA VERDAYANI

20102276

PROGRAM STUDI S1 TEKNIK INFORMATIKA
FAKULTAS INFORMATIKA
INSTITUT TEKNOLOGI TELKOM PURWOKERTO
2024

LEMBAR PERSETUJUAN PEMBIMBING

ANALISIS *MALWARE* PADA *EVIL-DROID* MENGGUNAKAN APLIKASI TELEGRAM DENGAN METODE *REVERSE ENGINEERING*

MALWARE ANALYSIS ON EVIL-DROID USING TELEGRAM APPLICATION WITH REVERSE ENGINEERING METHOD

Dipersiapkan dan Disusun Oleh

NADYA SADIRA VERDAYANI

20102276

Fakultas Informatika

Institut Teknologi Telkom Purwokerto

Pada Tanggal: 11 Juni 2024

Pembimbing Utama,

(Wahyu Adi Prabowo, S.Kom., M.B.A., M.Kom)

NIDN. 0613038503

LEMBAR PENGESAHAN TUGAS AKHIR

ANALISIS *MALWARE* PADA *EVIL-DROID* MENGGUNAKAN APLIKASI TELEGRAM DENGAN METODE *REVERSE ENGINEERING*

MALWARE ANALYSIS ON EVIL-DROID USING TELEGRAM APPLICATION WITH REVERSE ENGINEERING METHOD

Disusun Oleh

NADYA SADIRA VERDAYANI

20102276

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tugas Akhir Pada

Selasa, 25 Juni 2024.

Penguji I,

Bita Parga Zen, S.Kom., M.Han.
NIDN. 0603089202

Penguji II,

Trihastuti Yuniati, S.Kom., M.T.
NIDN. 0602068902

Pembimbingan Utama,

Wahyu Adi Prabowo, S.Kom., M.B.A., M.Kom.
NIDN. 0613038503

Dekan,

Auliya Burhanuddin, S,Si., M.Kom.
NIK. 19820008

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertandatangan di bawah ini,

Nama Mahasiswa : Nadya Sadira Verdayani
NIM : 20102276
Program Studi : S1 Teknik Informatika

Menyatakan bahwa Tugas Akhir dengan judul berikut:
ANALISIS *MALWARE* PADA *EVIL-DROID* MENGGUNAKAN APLIKASI TELEGRAM DENGAN METODE *REVERSE ENGINEERING*

Dosen Pembimbing Utama : Wahyu Adi Prabowo, S.Kom., M.B.A., M.Kom
Dosen Pembimbing Pendamping : -

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Institut Teknologi Telkom Purwokerto maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan, dan penelitian Saya Sendiri, tanpa bantuan pihak lain kecuali arahan dari Tim 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 tanggungjawab Saya, bukan tanggungjawab Institut Teknologi Telkom Purwokerto.
5. Pernyataan ini Saya buat dengan sesungguhnya, apabila dikemudian 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.

Purwokerto, 11 Juni 2024,

Yang Menyatakan,

(Nadya Sadira Verdayani)

KATA PENGANTAR

Puji syukur peneliti panjatkan kehadirat Allah SWT yang telah memberikan rahmat serta hidayah-Nya sehingga peneliti dapat menyelesaikan penyusunan skripsi dengan judul "Analisis *Malware* Pada *Evil-Droid* Menggunakan Aplikasi Telegram Dengan Metode *Reverse Engineering*" sebagai salah satu persyaratan yang harus dipenuhi untuk menyelesaikan Pendidikan tingkat Sarjana Komputer pada Fakultas Informatika Institut Teknologi Telkom Purwokerto.

Dalam penyusunan skripsi ini, tidak terlepas dari dukungan dan bantuan dari berbagai pihak selama ini. Oleh karena itu, pada kesempatan ini peneliti mengucapkan terimah kasih kepada:

1. Allah SWT yang senantiasa melimpahkan rahmat dan karunia-Nya sehingga skripsi ini dapat terselesaikan dengan baik;
2. Kedua orang tua peneliti, Bapak Fahrudin dan Ibu Suci Purwaningsih yang telah memberikan do'a, dukungan dan motivasi secara terus-menerus sehingga peneliti mampu menyelesaikan studinya sampai sarjana;
3. Dr. Tenia Wahyuningrum, S.Kom., M.T. selaku Rektor Institut Teknologi Telkom Purwokerto;
4. Auliya Burhanuddin, S.Si., M.Kom. selaku Dekan Fakultas Informatika Institut Teknologi Telkom Purwokerto;
5. Amalia Belandinna Arifa, S.Pd., M.Cs. selaku Ketua Program Studi S1 Informatika;
6. Wahyu Adi Prabowo, S.Kom., M.B.A., M.Kom. selaku dosen pembimbing pertama yang senantiasa memberikan pengarahan dan dukungan dalam menyelesaikan tugas akhir ini;
7. Seluruh dosen dan karyawan Institut Teknologi Telkom Purwokerto yang telah memberikan banyak kesempatan, tempat dan waktu pada peneliti dalam menyelesaikan studi di Institut Teknologi Telkom Purwokerto;
8. Keluarga dan saudara-saudara saya yang telah memberikan doa, semangat dan menjadi motivasi peneliti;

9. Fredo Nurasta Supriyadi, Joewandewa Yuliansyah, Adi Wardoyo, dan Muhammad Aunillah Alghifari yang telah menjadi teman yang telah memberikan motivasi serta dukungan dan juga menemani dalam penyusunan laporan penelitian;
10. Teman – teman peneliti, terutama Amira Cahyaning Putri, Dwi Indah Nurhaliza, Alysa Saufika Ananda, Nabila Rizky Prayunda, Siti Nur Kholifah, Putri Pangestu Gusti Ibna Al-Ayyubi, beberapa teman lainnya yang telah memberikan dukungan dan semangat.

Peneliti menyadari bahwa masih banyak kekurangan dalam penyusunan skripsi ini, sehingga kritik dan saran yang membangun sangat diharapkan. Akhir kata, peneliti berharap semoga skripsi ini dapat bermanfaat dan membantu menambah pengetahuan bagi yang membutuhkan.

Purwokerto, 26 Juni 2024

Nadya Sadira Verdayani

DAFTAR ISI

TUGAS AKHIR ..... **i**

LEMBAR PERSETUJUAN PEMBIMBING .....Error! Bookmark not defined.

LEMBAR PENGESAHAN TUGAS AKHIR .....Error! Bookmark not defined.

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR ..Error! Bookmark not defined.

KATA PENGANTAR ..... **iv**

DAFTAR ISI ..... **vii**

DAFTAR GAMBAR ..... **x**

DAFTAR TABEL ..... **xii**

DAFTAR SINGKATAN ..... **xiii**

DAFTAR LAMPIRAN ..... **xiv**

ABSTRAK ..... **xv**

ABSTRACT ..... **xvi**

BAB I PENDAHULUAN **1**

1.1 Latar Belakang **1**

1.2 Rumusan Masalah **3**

1.3 Pertanyaan Penelitian **3**

1.4 Tujuan Penelitian **3**

1.5 Batasan Masalah **4**

1.6 Manfaat Penelitian **4**

BAB II TINJAUAN PUSTAKA **5**

2.1 Penelitian Terkait **5**

2.2 Dasar Teori **10**

2.2.1 Android 10

2.2.2 Malware 10

2.2.3 Backdoor 12

2.2.4 Payload 12

2.2.5 Meterpreter 13
2.2.6 Evil-Droid 13
2.2.7 JADX 13
2.2.8 MobSF 13
2.2.9 Telegram 14
2.2.10 *Reverse Engineering* 14
BAB III METODOLOGI PENELITIAN 16
3.1 Objek dan Subjek Penelitian 16
3.2 Alat dan Bahan Penelitian 16
3.3 Diagram Alur Penelitian 17
3.3.1 Identifikasi Masalah 17
3.3.2 Studi Literatur 18
3.3.3 Tahap Pengujian 18
3.3.4 Tahap Analisis 20
BAB IV HASIL DAN PEMBAHASAN 21
4.1 Hasil Instalasi Pada Versi Android 21
4.1.1 Hasil Instalasi Android Versi 11 21
4.1.2 Hasil Instalasi Pada Android Versi 10 22
4.2 Hasil Instalasi Pengujian dan Analisis Metasploit 22
4.2.1 Pilihan *tools Evil-droid* 22
4.2.2 Konfigurasi LHOST 23
4.2.3 Konfigurasi LPORT 23
4.2.4 Membuat *Payload* 24
4.2.5 Memilih *Payload* 24
4.2.6 Memilih target aplikasi 24
4.2.7 Menyisipkan *Malware* 25
4.2.8 Pilihan *exploit* 25
4.2.9 *Exploit* 25
4.3 Hasil Analisis Statis menggunakan MobSF 27
4.3.1 *Security Score* 27
4.3.2 Analisis *Permission* 29
4.3.3 Analisis *Source Code* 31

4.4 Hasil Analisis Manual menggunakan JADX 35
4.4.1 META-INF 35
4.4.2 Asset 36
4.4.3 Lib 36
4.4.4 Res 37
4.4.5 Resources.arsc 37
4.4.6 Classes.dex 38
4.4.7 Analisis *Permission* 38
4.4.8 Analisis *Source Code* 42
4.5 Perbandingan Analisis Manual dan Analisis Otomatis 47
BAB V KESIMPULAN DAN SARAN 50
5.1 Kesimpulan 50
5.2 Saran 51
DAFTAR PUSTAKA 52
LAMPIRAN 54

DAFTAR GAMBAR

Gambar 1.1 Contoh data *Malware* DStationX 1
Gambar 2.1 Metode *Reverse Engineering* 14
Gambar 3.1 Diagram Alur Penelitian 17
Gambar 4.1 Instalasi Android versi 11 21
Gambar 4.2 Instalasi Android versi 10 22
Gambar 4.3 Pilihan *tools evil-droid* 22
Gambar 4.4 Konfigurasi LHost 23
Gambar 4.5 Konfigurasi LPort 23
Gambar 4.6 Membuat *payload* 24
Gambar 4.7 Memilih *payload* 24
Gambar 4.8 Target aplikasi 24
Gambar 4.9 Hasil *backdoor* 25
Gambar 4.10 Pilihan *exploit* 25
Gambar 4.11 *Setting exploit* 26
Gambar 4.12 Mengirim pesan 26
Gambar 4.13 Membaca pesan 26
Gambar 4.14 Menerima pesan 26
Gambar 4.15 Membaca riwayat panggilan 27
Gambar 4.16 Menerima riwayat panggilan 27
Gambar 4.17 Skor keamanan *original* apk 28
Gambar 4.18 Skor keamanan ditanamkan *malware* 28
Gambar 4.19 *Scan file original* apk 32
Gambar 4.20 *Scan file* sesudah disisipi 32
Gambar 4.21 *Launcher Activity* 33
Gambar 4.22 Verifikasi sertifikat *server* 33
Gambar 4.23 Kode *original CameraView* 34
Gambar 4.24 Penambahan kode *CameraView* 34
Gambar 4.25 Perbedaan META-INF 35
Gambar 4.26 Contoh dalam *folder assets* 36
Gambar 4.27 Isi *folder lib* 36
Gambar 4.28 Isi *folder res* 37

Gambar 4.29 Isi *folder* resources.arsc 37
Gambar 4.30 *File* classes.dex 38
Gambar 4.31 *Original* AndroidManifest 39
Gambar 4.32 *AndroidManifest* Setelah disisipi *malware* 39
Gambar 4.33 Isi *folder stage* 43
Gambar 4.34 Isi *class MainBroadcastReceiver* 44
Gambar 4.35 Memastikan *MainService* 45
Gambar 4.36 Memulai tugas menjalankan *service* 45
Gambar 4.37 *Launcher Activity* 46
Gambar 4.38 Menjaga perangkat aktif 47
Gambar 4.39 Proses yang dapat diakses oleh telegram 47

DAFTAR TABEL

Tabel 2.1 Penelitian Terkait 8
Tabel 3.1 Kebutuhan Perangkat Keras 16
Tabel 3.2 Kebutuhan Perangkat Lunak 17
Tabel 4.1 Penambahan sesudah disisipi MobSF 29
Tabel 4.2 Penambahan sesudah disisipi JADX 39
Tabel 4.3 Perbandingan *Permission* 48

DAFTAR SINGKATAN

MOBSF	*= Mobile Security Framework*
APK	*= Android Package Kit*
HTTP	*= Hypertext Transfer Transfer Protocol*
HTTPS	*= Hypertext Transfer Protocol Secure*
TCP	*= Transmission Control Protocol*
HTML	*= HyperText Markup Language*
XML	*= Extensible Markup Language*
API	*= Application Programming Interface*
UI	*= User Interface*
Malware	*= Malicious Software*
SMS	*= Short Message Service*

DAFTAR LAMPIRAN

Lampiran 1. Hasil *Exploit* ketika dijalankan 54
Lampiran 2. Permission JADX sebelum disisipi *malware* 57
Lampiran 3. Permissions JADX sesudah disisipi *malware* 59
Lampiran 4. Permissions MobSF sebelum disisipi *malware* 63
Lampiran 5. Permissions MobSF sesudah disisipi *malware* 65
Lampiran 6. Penambahan *class* a secara *manual* 67
Lampiran 7. Penambahan *class* b secara *manual* 68
Lampiran 8. Penambahan *class* c secara *manual* 70
Lampiran 9. Penambahan *class* d secara *manual* 70
Lampiran 10. Penambahan *class* e secara *manual* 71
Lampiran 11. Penambahan *class* f secara *manual* 71
Lampiran 12. Penambahan *class* g secara *manual* 73
Lampiran 13. Penambahan *class MainBroadcastReceiver* secara manual 73
Lampiran 14. Penambahan *class MainService* secara manual 73
Lampiran 15. Penambahan *class payload* secara *manual* 74
Lampiran 16. *Source code* yang ditemukan hasil *otomatis* 84