ANALISIS INFEKSI MALWARE ANDROID APLIKASI COVID-19 DENGAN METODE REVERSE ENGINEERING

SKRIPSI

Disusun oleh:

Deris Wahyu Nurdiarto
17.83.0058

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2020

ANALISIS INFEKSI MALWARE ANDROID APLIKASI COVID-19 DENGAN 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:

Deris Wahyu Nurdiarto
17.83.0058

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2020

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS INFEKSI MALWARE ANDROID APLIKASI COVID-19 DENGAN METODE REVERSE ENGINEERING

yang dipersiapkan dan disusun oleh

Deris Wahyu Nurdiarto

17.83.0058

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 21 Desember 2020

Dosen Pembimbing,

Joko Dwi Santoso, M.Kom
NIK. 190302181

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS INFEKSI MALWARE ANDROID APLIKASI COVID-19 DENGAN METODE REVERSE ENGINEERING

yang dipersiapkan dan disusun oleh

Deris Wahyu Nurdiarto

17.83.0058

Telah dipertahankan di depan Dewan Penguji
pada tanggal 17 Desember 2020

Susunan Dewan Penguji

Nama Penguji	**Tanda Tangan**
Joko Dwi Santoso, M.Kom **NIK. 190302181**	_____
Dony Ariyus, M.Kom **NIK. 190302128**	_____
Agung Nugroho, M.Kom **NIK. 19030241**	_____

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 21 Desember 2020

DEKAN FAKULTAS ILMU KOMPUTER

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

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Deris Wahyu Nurdiarto
NIM : 17.83.0058

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Infeksi Malware Android Aplikasi Covid-19 Dengan 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, 17 Desember 2020

Yang Menyatakan,

Deris Wahyu Nurdiarto

HALAMAN MOTTO

"Hidup tidak mensyaratkan bahwa kita harus menjadi yang terbaik --- hanya bahwa kita harus berupaya sebaik mungkin"
(H. Jackson Brown Jr)

"Setiap aksi pasti dihadapkan pada reaksi yang sebanding"
(Sir Isaac Newton)

"Bersabarlah. Anda akan tahu kapan saat Anda harus bangun dan bergerak maju"
(Ram Dass)

"Kelemahan kita yang terbesar terletak dalam menyerah, cara yang paling pasti untuk meraih sukses adalah dengan selalu mencoba sekali lagi"
(Thomas Edison)

"Orang yang paling kaya adalah dia yang puas dengan apa yang dimilikinya"
(Robert C. Savage)

"Belajarlah melepaskan, itulah kunci untuk meraih kebahagiaan"
(Sang Buddha)

HALAMAN PERSEMBAHAN

Segala puji bagi Allah SWT atas limpahan rahmat dan hidayah serta karunia-Nya sehingga skripsi ini selesai dengan sebaik-baiknya. Skripsi ini saya persembahkan untuk :

1. Kedua orang tua, Bapak Suharto dan Ibu Sri Budiharti yang selalu mendoa'kan, 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 skripsi ini.
3. Kepada Bibi saya Sri Sayekti dan kakak serta adik saya yang selalu memberikan semangat dan dukungan.
4. Kepada sahabat dan teman-teman yang ada disaat suka maupun duka selama masa perkuliahan saya.
5. Sesorang yang sangat berharga dan memberikan banyak arti dalam hidup saya, Dinda Ajeng Ciptarany. Terima kasih atas cinta, dukungan, kebaikan, perhatian, dan kebijaksanaan serta telah mengajarkan arti kedewasaan.

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 "Analisis Infeksi Malware Android Aplikasi Covid-19 dengan Metode Reverse Engineering".

Skripsi ini disusun sebagai syarat memperoleh gelar Sarjana Komputer pada program Studi S1 Teknik Komputer 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 ini dengan baik dan semoga dapat memberikan mamfaat 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 Santoro, 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, 17 Desember 2020

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Coronavirus menjadi pandemi yang dirasakan dampaknya secara global di setiap negara. Selain ancaman kesehatan terdapat juga ancaman pada bidang teknologi yang dapat disebut sebagai *Cyberattack*. Ancaman *Cyberattack* dapat berupa *malware*, email *scam*, *ransomware*, dan *malicious domains*. *Smartphone* dengan sistem operasi *android* menjadi target utama dan banyak laporan berita yang menunjukkan serangan program berbahaya dengan memanfaatkan COVID-19 telah terjadi pada ribuan pengguna *smartphone*. *Malware* merupakan sebuah program jahat yang dikembangkan dengan tujuan menyusup dalam sistem operasi hingga dapat merusak atau mencuri informasi penting. Untuk mengetahui bagaimana *malware* dapat melakukan infeksi pada aplikasi *android* dengan tema COVID-19 maka perlu dilakukan analisis.

Analisis dilakukan dengan melakukan implementasi penyusupan *malware* pada sampel aplikasi menggunakan metode *reverse engineering*. Penyusupan *malware* pada sampel aplikasi menggunakan teknik *repackaging attack*. Dalam melakukan *repackaging attack*, aplikasi akan dilakukan *reverse engineering* dengan tujuan menyusupkan *payload* yang diciptakan menggunakan *framework Metasploit*. *Payload* akan bekerja menjadi *malware* yang dapat melakukan *exploit*.

Hasil implementasi yaitu *file* apk aplikasi COVID_19 yang berhasil di infeksi *malware*. Selanjutnya dilakukan analisis statis dan analisis dinamis guna mengetahui dampak dari hasil infeksi *malware*. Analisis statis menggunakan *tool* VirusTotal dan Framework MobSF. Pada *tool* VirusTotal 19 dari 60 *anti-malware* berhasil mendeteksi *malware* pada COVID_19.apk, selanjutnya ditemukan perbedaan ukuran *file* dan SHA256 dari sebelum infeksi *malware*. Framework MobSF dengan fitur *static analyzer* yaitu *Permission* berhasil mendeteksi perbedaan. Hasil analisis dinamis *malware* berhasil dijalankan dengan proses *exploit* yang mendapat akses perangkat *android*. Aplikasi COVID_19 juga mendapatkan peringatan sebagai program berbahaya dari Google Play Protect.

Kata kunci: Android, APK, Malware, Analisis Statis, Analisis Dinamis

ABSTRACT

Coronavirus has become a pandemic whose impact is felt globally in every country. In addition to health threats, there are also threats in the technology sector which can be referred to as cyber attacks. Cyberattack threats can include malware, email scams, ransomware, and malicious domains. Smartphones with the Android operating system are the main target and many news reports indicate attacks by malicious programs using COVID-19 have occurred in thousands of smartphone users. Malware is a malicious program developed to infiltrate the operating system so that it can destroy or steal important information. To find out how malware can infect an android application with the theme COVID-19, an analysis is needed.

The analysis was carried out by implementing malware infiltration in the sample application using the reverse engineering method. Infiltration of malware in the sample application uses the repackaging attack technique. In carrying out a repackaging attack, the application will be reverse engineering to insert the payload created using the Metasploit framework. The payload will work as an exploitable malware.

The results of the implementation are the COVID_19 application apk file that was successfully infected with malware. Furthermore, static analysis and dynamic analysis are carried out to determine the impact of the results of malware infection. Static analysis using VirusTotal tool and MobSF Framework. In the VirusTotal tool 19 out of 60 anti-malware successfully detected malware on COVID_19.apk, then found differences in file size and SHA256 from before malware infection. The MobSF framework with static analyzer features, namely Permission successfully detects differences. The results of the dynamic analysis of malware were successfully executed with an exploit process that had access to an Android device. The COVID_19 app also received a warning as a malicious program from Google Play Protect..

Keyword: *Android, APK, Malware, Static Analysis, Dynamic Analysis*