ANALISIS COVIDLOCK RANSOMWARE MENGUNAKAN METODE HYBRID ANALISIS

SKRIPSI

diajukan oleh

Hari Setiawan

17.83.0025

PROGRAM SARJANA

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

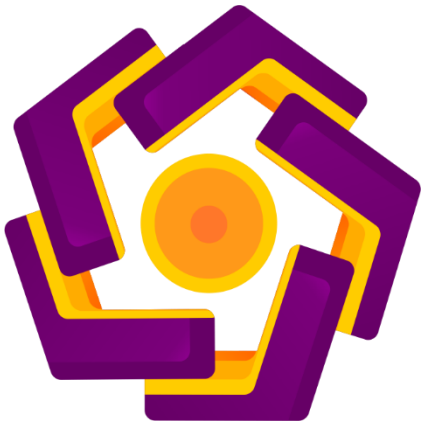
2022

ANALISIS COVIDLOCK RANSOMWARE MENGUNAKAN METODE HYBRID ANALISIS

HALAMAN JUDUL

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



diajukan oleh

Hari Setiawan

17.83.0025

PROGRAM SARJANA

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS COVIDLOCK RANSOMWARE MENGUNAKAN METODE HYBRID ANALISIS

yang disusun dan diajukan oleh

Hari Setiawan

17.83.0025

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 25 Juli 2022

Dosen Pembimbing,

Wahyu Sukestyastama Putra, S.T., M.Eng.

NIK. 190302328

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS COVIDLOCK RANSOMWARE MENGUNAKAN METODE HYBRID ANALISIS

yang disusun dan diajukan oleh

Hari Setiawan

17.83.0025

Telah dipertahankan di depan Dewan Penguji
pada tanggal 25 Juli 2022

Susunan Dewan Penguji

Nama Penguji	**Tanda Tangan**
Wahyu Sukestyastama Putra, S.T., M.Eng **NIK. 190302328**	_____
Melwin Syafrizal, S.Kom., M.Eng. **NIK. 190302105**	_____
Rini Indrayani, S.T., M.Eng. **NIK. 190302417**	_____

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 25 Juli 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Hari Setiawan
NIM : 17.83.0025

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Covidlock Ransomware Mengunakan Metode Hybrid Analisis

Dosen Pembimbing : Wahyu Sukestyastama Putra, S.T., M.Eng.

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, 26 Juli 2022

Yang Menyatakan,

Hari Setiawan

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 Wahyu Sukestyastama Putra, S.T., M.Eng. 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.

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 selesaianya 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. Bapak Hanif Al Fatta, M.Kom 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 Wahyu Sukestyastama Putra, S.T., M.Eng. 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.

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

Wassalamualaikum Warahmatullahi Wabarakatuh

Yogyakarta, 8 Juli 2022

Hari Setiawan

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Coronavirus menjadi pandemic yang dirasakan dampaknya secara global di setiap negara. Selain ancaman kesehatan terdapat juga ancama dalam bidang teknologi yang disebut sebagain *Cyberattack.* Ancaman *Cyberattack* dapat berupa *malware, email scam, ransomware,* dan *malicious domains.* meningkatnya isu wabah Covid-19 hal ini dimanfaatkan oleh *threat actor* dengan menyebarkan aplikasi terkait *utilitas* Covid-19 namun telah ditambahkan fungsi *malicious.* Salah satunya melalui aplikasi *mobile* bernama *Corona Virus Tracker* yang diunduh melalui domain *coronavirusapp.site.*

Aplikasi *Corona Virus Tracker* berfungsi sebagai aplikasi *tracking* area yang terdampak Covid-19. Ketika setelah di instal, aplikasi akan meminta *permission* antara lain yaitu *lockscreen* dan *ignore battery optimization. Ignore Battery Optimization* digunakan sebagai metode *persistence* dengan mengabaikan kondisi baterai yang lemah untuk mematikan aplikasi. *Permission lockscreen* digunakan *threat actor* untuk mengenkripsi perangkat korban, ketika aplikasi telah berhasil di instal.

Analisis dilakukan dengan mengunakan metode *reverse engineering*. dalam melakukan *reverse engineering* mengunakan tools *apktool, jd-gui, dan Dex2jar*. Aplikasi *Corona Tracker* termasuk ke dalam *mobile ransomware* dengan kunci *offline*. Kunci dekripsi dapat ditemukan di dalam baris kode aplikasi (*hard encoded*) yaitu 4865083501.

Kata kunci: *Coronavirus, Android, Ransomware, Kalilinux*

Abstract

Coronavirus is a pandemic that is being felt globally in every country. In addition to health threats, there are also threats in the field of technology called Cyberattack. Cyberattack threats can include malware, email scams, ransomware, and malicious domains. The increasing issue of the Covid-19 outbreak has been exploited by threat actors by spreading applications related to the Covid-19 utility, but malicious functions have been added. One of them is through a mobile application called Corona Virus Tracker which is downloaded via the coronavirusapp.site domain.

The Corona Virus Tracker application functions as a tracking application for areas affected by Covid-19. Once installed, the application will ask for permissions, including lockscreen and ignore battery optimization. Ignore Battery Optimization is used as a persistence method by ignoring low battery conditions to kill applications. Permission lockscreen is used by threat actors to encrypt the victim's device, when the application has been successfully installed.

The analysis was carried out using the reverse engineering method. in doing reverse engineering using tools apktool, jd-gui, and Dex2jar. Corona Tracker application belongs to mobile ransomware with offline lock. The decryption key can be found in the application code line (hard encoded) which is 4865083501.

***Keywords**: Coronavirus, Android, Ransomware, Kalilinux*