eISSN : 2621-4970
pISSN : 2621-4962

Volume 3 | No 2
Juli | **2020**

Analisis Aplikasi Malware pada Android dengan Metode Statik

Samuel Sinambela[1], Aditya Robbi Pangestu[2], Rangga Feriyanto[3]
[1,2,3]Fakultas Ilmu Komputer, Program Studi Teknik Komputer
Universitas Amikom Yogyakarta
samuel.sinambela@students.amikom.ac.id

Abstrak

Terkadang pengguna android tidak hati-hati saat berselancar diinternet dan tanpa sadar sebuah malware telah terinstal di perangkat mereka. Malware inilah yang nantinya akan menjadi jalan bagi penyerang untuk mengambil sesuatu di perangkat korban. Maka dari itu, diperlukannya analisis untuk mengetahui apa saja akses yang dibutuhkan ketika sebuah Malware terunduh di perangkat korban. Tujuan Penelitian adalah untuk menganalisis mendapatkan informasi malware yang terdapat pada aplikasi. Metode yang dipakai dalam penelitian ini menggunakan metode kuantitatif. Sample malware akan diambil melalui iklan dan menganalisis malware tersebut menggunakan metode analisis static yang hanya membaca informasi malware tanpa harus menginstalnya. Hasil dari analisis, terdeteksi Malware dan memiliki perizinan yang tidak pada tempatnya. Seperti yang terlihat, aplikasi game tidak memerlukan izin untuk melihat panggilan yang berlangsung. Maka dari itu, diperlukannya kejelian pengguna agar tidak sembarangan mengunduh atau mengklik sesuatu ketika berinternet. User juga harus update pada keamanan perangkat yang dimiliki.

Kata kunci: Malware, Analisis Statik, Android

Abstract

Sometimes Android users are not careful when surfing the internet and unknowingly have malware installed on their devices. This malware is what will later become a way for attackers to take something on the victim's device. Therefore, analysis is needed to see what access is needed when malware is downloaded on the victim's device. The research objective is to analyze the malware information contained in the application. The method used in this research is quantitative methods. Malware samples will be taken through advertisements and analyze the malware using a static analysis method that only reads malware information without having to install it. As a result of the analysis, the malware was detected and had inappropriate permissions. As you can see, the game application is not allowed to see the ongoing calls. Therefore, users need carefulness, so they do not download or click something when surfing the internet. Users also have to update on their own devices.

Keywords: *Malware, Static Analysis, Android*

PENDAHULUAN

Pada saat ini banyak sekali teknologi yang sudah berkembang pesat, salah satunya adalah banyaknya software-software yang membantu memudahkan kita dalam pekerjaan sehari-hari seperti berkomunikasi lewat whatsapp atau email dan sebagainya. Namun terkadang ada seseorang yang memiliki niat tidak baik dengan menyisipkan sebuah kode pada aplikasi tersebut agar dapat mengambil informasi yang ada pada perangkat kita [1].

Malware analisis merupakan salah satu cara untuk memperoleh informasi yang ada pada sebuah malware agar dapat mengatasi serangan sebuah malware pada user yang

terkena serangan malware, oleh karna itu kami disini akan menganalisis salah satu malware pada sebuah aplikasi yang berada pada system operasi android dengan menggunakan metode analisis statik [2].

Banyak malware yang tersebar saat ini seperti, virus, Trojan, spyware, dan masih banyak lainnya malware ini sangat lah berbahaya bagi kita karena dapat mengganggu fungsi perangkat kita mulai dari mengambil data sampai perangkat kita tidak dapat di gunakan lagi.

Malware merupakan sebuah kode yang ada pada perangkat lunak yang menyebabkan kerusakan pada fungsi sistem [3]. Malware menjadi ancaman yang sangat berbahaya dan menyebabkan masalah pada korban yang terkena, karna hal ini keamanan internet sangatlah penting dalam zaman ini yang dimana internet telah menjadi salah satu kebutuhan primer.

Rumusan Masalah

Adapun rumusan masalah kali ini adalah Bagaimana untuk meneliti sebuah aplikasi telah terisi malware.

Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Untuk menganalisis malware yang terdapat pada aplikasi.
2. Mendapat informasi malware yang ada dalam aplikasi.

Manfaat Penelitian

Manfaat dari penelitian ini adalah memberikan informasi malware yang ada dalam aplikasi agar pengguna dapat mengetahui bagaimana sebuah aplikasi malware mencoba masuk lewat perizinan yang janggal sehingga pengguna dapat berhati-hati dan tidak sembarangan dalam mengklik atau membuka sesuatu yang janggal saat berinternet.

Tinjauan Pustaka

Pada penelitian sebelumnya, Rifyandaru Wibisono, Avon Budiono, S.T., M.T. dan Ahmad Almaarif., S.Kom., M.T. yang berjudul "ANALISIS MALWARE PADA SISTEM OPERASI ANDROID MENGGUNAKAN MEMORY FORENSICS BERDASARKAN API" menganalisa 10 malware untuk dianalisis menggunakan volatility dan tool APK untuk memberikan dampak menggunakan hasil dari analisis dan juga berdasarkan aktifitas malware dari API. Hasil dari penelitian tersebut adalah dampak yang berkaitan dengan API dan hasil analisisnya [8].

Kemudian penelitian Leidy Kurnia Hatika, Avon Budiyono dan Ahmad Almaarif yang berjudul "ANALISIS KETEPATAN DETEKSI MALWARE PADA SOFTWARE ANTIVIRUS MENGGUNAKAN METODE ANALISIS STATIS" menganalisa malware yang berfokus pada nilai string lalu dibandingkan dengan karateristik malware berdasarkan hasil pemindaian terbanyak dari aplikasi antivirus [9].

LANDASAN TEORI

Malicious Software

Malicious Software atau *Malware* merupakan sebuah perangkat lunak yang dibuat untuk menyerang, ataupun merusak sistem komputer. Malware biasanya disispkan pada sebuah file ataupun aplikasi yang di buat untuk mengelabui korban agar tidak terdeteksi oleh korban untuk mengambil informasi rahasia dari korban

ataupun untuk merusak system yang ada pada prangkat korban.

Jenis-Jenis malware

Ada beberapa jenis malware yang perlu diketahui [4], antara lain:

1. Trojan merupakan salah satu jenis malware yang disisipkan pada aplikasi. Tujuan trojan biasanya untuk mencuri data yang terdapat pada perangkat korban tanpa di ketahui dengan cara mendapat akses untuk mengambil informasi yang ada pada perangkat korban.
2. Worm merupakan salah satu jenis malware yang menyerang lewat jaringan dengan cara mengirimkan file yang telah tersisipkan worm ini kepada penerima lewat jaringan. Worm dapat menggandakan dirinya sendiri pada sistem komputer. Sebuah worm memanfaatkan celah keamanan pada jaringan untuk menyebarkan dirinya.
3. Spyware merupakan salah satu jenis malware yang bekerja sebagai mata-mata untuk memata-matai pengguna komputer dan mengirimkan informasi pada pihak yang mengirimkan spyware tersebut.
4. Adware merupakan salah satu jenis malware yang disisipkan kedalam aplikasi, malware ini akan menampilkan pop-up iklan terus menerus. Biasanya malware ini terdapat pada aplikasi yang bersifat gratis.
5. Virus merupakan salah satu jenis malware yang menyerang file dan menggandakan dirinya sendiri. Ketika file yang terkena virus dijalankan bisanya virus menyebar lewat file yang disisipkan malware tersebut.
6. Keylogger merupakan sebuah program yang dibuat untuk memantau pengetikan pada keyboard yang kemudian nanti data yang terekam dapat dilihat oleh si pemasang keylogger tersebut.
7. Ransomware merupakan salah satu jenis malware yang membuat pengguna tidak bisa mengakses data korban pada perangkat komputernya dengan cara mengunci prangkat tersebut. Hingga korban membayar tebusan yang di pinta oleh pelaku ransomware.

Analisis Statik

Teknik analisis statik dijalankan tanpa mencoba menjalankan aplikasi pada prangkat android ataupun emulator. Analisis statik adalah teknik mengamati perilaku malware dengan cara menganalisis code segmen. Bentuk analisis statik akan menguraikan dan membongkar serta mencari pola mencurigakan yang ada di file ataupun aplikasi [5].

Android

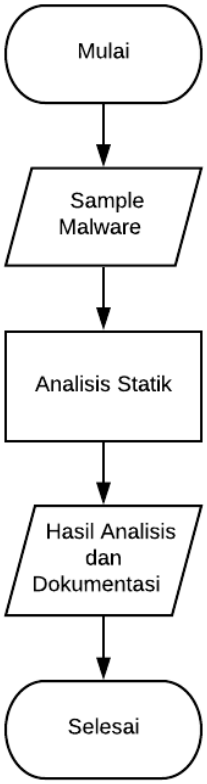
Android adalah salah satu system operasi yang ada pada perangkat seluler yang open source dan memiliki fitur lengkap yang di buat untuk melayani konsumen. Sifat open source pada android membuat banyak vendor dan berbagai merk handphone menggunakan system operasi ini [6].

Model keamanan pada system operasi android menggunakan system operasinya sendiri, seperti menambahkan permission pada file dalam sebuah aplikasinya. Pada prosesnya user akan mendapatkan pertanyaan sebelum menginstal sebuah aplikasi, apakah user akan memberikan permission yang diminta oleh aplikasi

tersebut. Fungsi tersebut digunakan untuk fungsi dari aplikasi sudah tepat atau belum [7].

METODE PENELITIAN

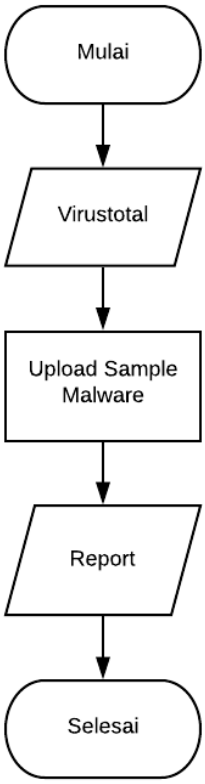
Metode yang dipakai dalam penelitian ini menggunakan metode kuantitatif. Sample malware akan diambil melalui iklan dan menganalisis malware tersebut menggunakan metode analisis statik. Hasil yang didapat akan menunjukkan bagaimana perilaku malware serta informasi yang ada pada malware tersebut. Berikut adalah alur penelitian yang akan dilakukan:



Gambar 1. Alur penelitian

ANALISIS DAN PERANCANGAN

Metode analisis malware yang dipakai dalam penelitian ini adalah metode analisis statik dengan alur sebagai berikut:



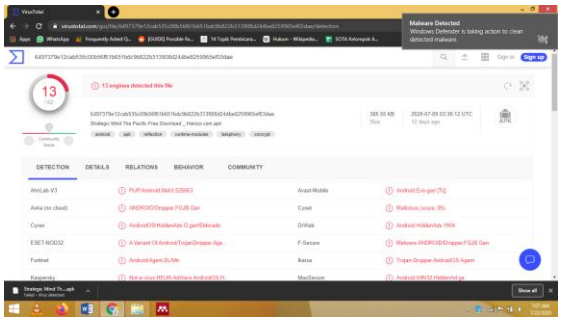
Gambar 2. Alur analisis statik

Perincian alurnya adalah mempersiapkan website scanning seperti virustotal.com. Kemudian mencari sample malware dari iklan-iklan dan menguploadnya ke virustotal. Hasil report yang didapat nantinya akan diteliti lebih lanjut.

IMPLEMENTASI DAN PEMBAHASAN

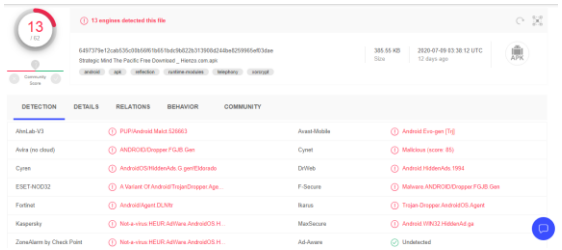
Pengujian kali ini menggunakan website virustotal.com untuk menganalisis aplikasi android yang telah didapatkan dari iklan.

Aplikasi game yang diunduh bernama *Strategic Mind The Pacific Free Download – Hienzo.com.apk*. Kami mencoba mendownload dengan windows defender yang aktif, namun apk tersebut terdeteksi berbahaya. Maka dari itu, kami mengunduhnya tanpa windows defender dan berikut informasi yang kami dapat dari hasil scanning virustotal.



Gambar 3. Mengunduh aplikasi malware dengan windows defender

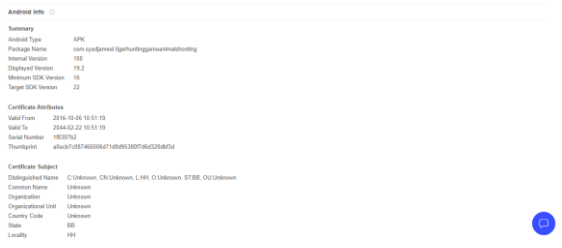
Terdapat 13 engine berbahaya yang terdeteksi di masing-masing antivirus seperti berikut:



Gambar 4. Hasil scanning

Detail aplikasi tersebut sebagai berikut:

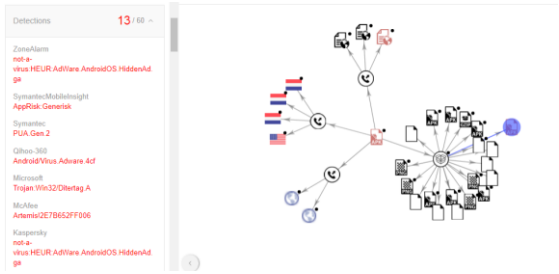
Gambar 5. Detail aplikasi malware



Gambar 6. Detail aplikasi malware

Terlihat bahwa aplikasi tersebut memiliki hubungan ke beberapa URL, domain, serta IPs yang berbeda-beda. Berikut juga relasi dari aplikasi ini:

Gambar 7. Hubungan aplikasi malware

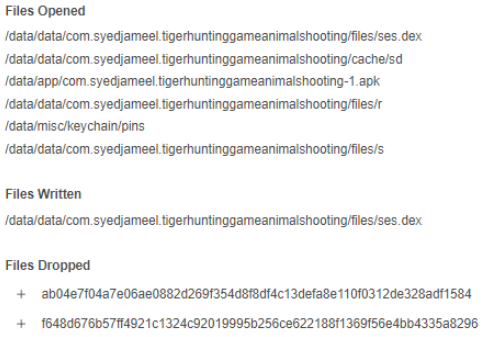


Gambar 8. Relasi aplikasi malware ke berbagai tempat

Adapun perilaku dari aplikasi ini ketika dieksekusi, cukup banyak. Begitu juga dengan traffic ip ke beberapa tempat:

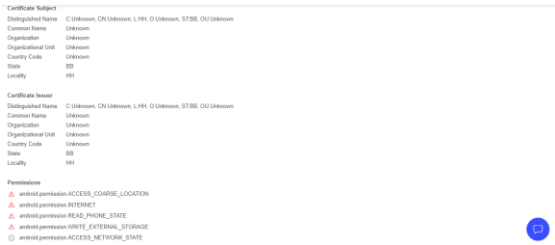
Gambar 9. Informasi perilaku aplikasi malware saat dieksekusi

Terlihat aplikasi ini pun dapat menjalankan ke beberapa file system:



Gambar 10. Proses aplikasi malware menuju file system

Saat terinstal, aplikasi ini meminta beberapa perizinan yang diperlukan agar terhubung penuh ke perangkat korban



Gambar 11. Perizinan aplikasi malware

Pada bagian perizinan, terlihat bahwa aplikasi ini memiliki perizinan *android.permission.READ_PHONE_STATE* yang berarti dapat melihat informasi jaringan pengguna, panggilan berlangsung, dan akun yang tertaut di hp pengguna. Aplikasi ini juga terdeteksi beberapa malware yang dapat menginstal program berbahaya tanpa sepengetahuan user. Malware yang terdapat dalam aplikasi ini serta perizinan yang mencurigakan, membuat aplikasi ini berbahaya bagi pengguna, jika pengguna tidak teliti pada saat menginstal ke perangkatnya.

KESIMPULAN

Aplikasi yang didapat melalui iklan-iklan pada website yang tidak terpercaya, biasanya mengandung malware. Terlihat bahwa aplikasi yang kami dapat melalui iklan, terdeteksi malware dan memiliki perizinan yang tidak pada tempatnya. Seperti yang terlihat, aplikasi game tidak memerlukan izin untuk melihat panggilan yang berlangsung. Maka dari itu, diperlukannya kejelian pengguna agar tidak sembarangan mengunduh atau mengklik sesuatu ketika berinternet. User juga harus update pada keamanan perangkat yang dimiliki. Tentunya hal ini dapat menjaga user dari bocornya informasi pribadi yang tertaut di perangkat pribadinya.

Saran

Berdasarkan hasil dari analisis yang telah dilakukan, saran yang dapat diberikan yaitu analisis malware dengan metode analisis statik juga dapat dilakukan melalui scanning antivirus. Lebih baik lagi jika dilakukan penggabungan 2 metode, yaitu analisis statik dan dinamis agar bisa mempelajari lebih dalam tentang malware yang berkembang dan juga pembuktian deteksi yang akurat.

DAFTAR PUSTAKA

[1] Solahudin Rusdi, A. (2019). *ANALISIS INFEKSI MALWARE PADA PERANGKAT ANDROID DENGAN METODE HYBRID ANALYSIS* (Doctoral dissertation, Universitas Siliwangi).

[2] Febrianto, A. F., Budiyono, A., & Almaarif, A. (2019). *Analisis Malware Pada Sistem Operasi Android Menggunakan Metode Network Traffic Analysis*. eProceedings of Engineering, 6(2).

[3] McGraw, G., & Morrisett, G. (2000). *Attacking malicious code: A report to the infosec research council. IEEE Software*, 17(5), 33-41.

[4] Utomo, Y. A., Ismail, S. J. I., & Zani, T. (2018). *Membangun Sistem Analisis Malware Pada Aplikasi Android Dengan Metode Reverse Engineering Menggunakan Remnux*. eProceedings of Applied Science, 4(3).

[5] Hatika, L. K., Budiyono, A., & Almaarif, A. (2019). *Analisis Ketepatan Deteksi Malware Pada Software Antivirus Menggunakan Metode Analisis Statis*. eProceedings of Engineering, 6(2).

[6] Febrianto, A. F., Budiyono, A., & Almaarif, A. (2019). *Analisis Malware Pada Sistem Operasi Android Menggunakan Metode Network Traffic Analysis*. eProceedings of Engineering, 6(2).

[7] Iman, A. N., Budiyono, A., & Almaarif, A. (2019). *Analisis Malware Pada Sistem Operasi Android Menggunakan Permission-based*. eProceedings of Engineering, 6(2).

[8] Wibisono, R., Budiyono, A., & Almaarif, A. (2019). *Analisis Malware Pada Sistem Operasi Android Menggunakan Memory Forensics Berdasarkan Api*. eProceedings of Engineering, 6(2).

[9] Hatika, L. K., Budiyono, A., & Almaarif, A. (2019). *Analisis Ketepatan Deteksi Malware Pada Software Antivirus Menggunakan Metode Analisis Statis*. eProceedings of Engineering, 6(2).