CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 1, No. 2, November 2018, hlm 62-66

Malicious Software Analysis

Wisnu Pranoto

[1] Magister Teknik Informatika Fakultas Teknologi Industri
Universitas Islam Indonesia, Jl. Kaliurang Km. 14,5 Sleman Yogyakarta
[1] Wisnunataa@gmail.com

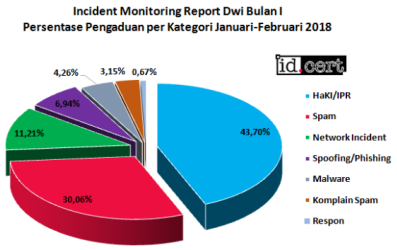
Abstrak

Abstrak–Analisis sebuah malware pada perangkat android yang terdapat pada aplikasi iCalender menggunakan teknik analisis static dan teknik komputer forensik. Penelitian ini sangat berguna agar user dapat mengenal aplikasi android lainnya dan menghindari masuknya malware pada mernagkat android milik user. Berbagai tahapan analisis pada aplikasi android dimulai dengan merename apk menjadi zip, kemudian mengkestrak file Zip menjadi format Dex. Filte Dex dikonvert menjadi file Jar menggunakan tool Dex2jar. Selanjutnya hasil file Jar didecomplie dengan tool JD-GUI untuk melihat source code java pada aplikasi iCalender, kemudian dianalisis.

Kata Kunci–Malware, Android, iCalender

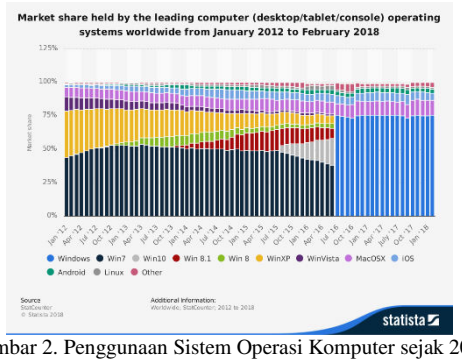
I. Pendahuluan

Analisis malware menjadi salah satu bagian terpenting dalam ilmu dasar digital forensik (Mesood, 2004). Dalam pekerjaan investigator untuk menganalis perangkat lunak berbahaya ini menjadi sebuah tantangan setiap melakukan penyelidikan. Hal tersebut disebabkan serangan malware meningkat signifikan berdasarkan penelitian dari ID-CERT yang menjadi laporan Dwi Bulan I 2018, diperoleh data terkait pengaduan *cybercrime* menyebutkan bahwa 4.26% serangan dari malware tersebut.



Gambar 1. Pengaduan Kategori *Cybercrime* Pada Januari-Febuari 2018

Malware atau *Malicious Software* adalah sebuah perangkat lunak yang bisa menyusup ke sistem operasi sehingga dapat menggangu sistem dan juga mengumpulkan informasi rahasia atau dapat mencuri file-file penting yang ada pada sistem. Berikut adalah statistik penggunaan sitem operasi komputer sejak tahun 2012 hingga 2018 :



Gambar 2. Penggunaan Sistem Operasi Komputer sejak 2012

Malware bekerja 75,43% di sistem operasi *windows*, dikarnakan sebagian besar penggunaan sistem operasi *windows* di dunia (statista.com, 2018). Malware bisa disisipkan melalui file-file umum seperti pengolahan kata (.doc), pengolahan angka (.xls) aplikasi (.exe) dan file lainnya. Malware bisa merupai dengan nama file yang umum digunakan bebagai keperluan, seperti data (.dat), driver (.drv), library (.lib) dan lain-lain. *Malicious software* melibatkan virus komputer, spyware (perangkat pengintai), adware (perangkat iklan), crimeware (perangkat jahat) dan juga software lainnya yang dapat berkeinginan jahat dan tidak diinginkan.

Perkembangan pada era sekarang teknologi pun menjadi ancaman berkembangnya malware-malware baru, sehingga mengakibatkan banyak pihak yang dirugikan, dikarenakan adanya serangan dari malware-malware tersebut. Bahkan hampir sistem operasi pun terjangkit oleh malware.

Pada saat ini teknologi semakin berkembang dan mulai memaparkan berbagai jenis *smartphone* dan tablet PC dengan berbagai jenis *platform windows*,

ios, android, dan sebagainya berdasarkan data yang didapat dari (StatCounterGlobalStats, 2017) penggunaan sistem operasi mobile di Indonesia menyebutkan bahwa 64,99% penggunaan sistem operasi android diperangkat *mobile smartphone*. Semakin banyaknya penggunaan *smartphone* maupun tablet PC oleh penggunanya, dikarenakan desain yang mewah, bentuk ukuran yang efisien, mudah untuk pengoprasiannya bagi semua kalangan, dan banyak lagi keunggulan dari *smartphone* dan tablet PC. Dalam hal ini penggunaan *mobile* di Indonesia mencapai 45% menurut penelitian dari (Hootsuite.com, 2018).

II. Literatur Review

Berikut ini akan dibahas beberapa ulasan terkait penelitian yang telah dilakukan sebelumnya yang relevan dan berhubungan dengan malware.

Dimulai dari penelitian yang dilakukan oleh (P.V.Shijo, A. Salim, 2015) yang melakukan analisis statis dan dinamis untuk mendeteksi malware menggunakan *tools analyzer* cuckoo pada platform ubuntu dengan menggunakan virtual mesinware, bertujuan apakah adanya malware atau tidak.

Kemudian yang dilakuan oleh (Feizollah, etc 2016) yang mempelajari mendeteksi malware android dengan efektivitas intent untuk mengetahui keamanan *smartphone* dengan melakukan analisis statis menggunakan kurva *Receiver* Operating *Characteristic* untuk mengukur kinerja dalam mendeteksi instruksi dan mendapatkan perbandingan.

Penelitian selanjutnya yang dilakukan oleh (Hampton, Baig, Zeadally, 2018) melakukan perbandingan 14 jenis ransomware yang terinfeksi pada palatform Windows dan melakukan perbandingan Windows Application Programming Interface.

Kemudian penelitian yang dilakukan oleh (Kabakus, Dogru, 2018) melakukan teknik analisis statis dan dinamis pada *platform* android hybrid untuk mencari karakteristik malware pada android.

III. Malicious Software

Malicious Software singkatnya bagi orang advance dalam teknologi informasi menyebutnya Malware, yang merupakan perangkat lunak berbahaya yang diciptakan untuk menyusup, mencuri atau merusak sistem perangkat komputer.

Perangkat lunak yang terindifikasi sebagai perangkat yang merusak berdasarkan maksud dan tujuan tertentu bagi pencipta malware. Terkait dalam jenis malware virus , trojan horse, worm, spyware, wabbit, keylogger, dan berbagai jenis malware lainnya. Berdasarkan pengetahun yang diperoleh ilmu forensik meliputi teknik metode seperti time stamping, entropy analysis (tipe file, hashing, dll) untuk mengenali pola malware, ada beberapa karakteristik malware [2]. berikut adalah karakteristik malware :

1. *Time stamping*
   Metode ini menganalisis durasi antara serangan dan tahap awal penyelidikan saat malware terinfeksi.
2. *Entropy analysis*
   File yang sering terinfeksi adalah file .exe karna sulit untuk dideteksi. Mungkin tersembunyi didalam indeks, mendaur ulang bins (sampah) atau folder sistem. Conohnya dari hal Windows/system32.
3. *Keyword and identifiers*
   Cara termudah untuk mengidentifikasi kode malware melalui kata kunci, yang disebut '*identifiers'* pengidentifikasi. Untuk memproleh data dari alamat IP, alamat email dan sumber-sumber lain untuk mendapatkan informasi yang diperlukan disebut pola komunikasi. Contohnya "key log" dapat berubah string digunakan untuk mencari petunjuk mengenai serangan malware pada sistem.

   Sebagian besar metode analisis malware menggunakan teknik statis dan dinamis. Fitur statis teruama terfokus dari kode biner, sedangkan fitur dinamis yang diambil dari urutan system call. Berikut adalah penjelas dari teknik statis dan dinamis [3] :

1. Malware Analisis Statis
   Menggunakan motode analisis statis ini di tuntut mampu memahami bahasa mesin terutama arsitektur sebuah program karena akan sangat membantu dalam menganalisis urutan kode-kode program malware terkait dengan mengumpulkan informasi dari prilaku sebuah malware.
2. Malware Analisis Dinamis
   Sedangkan Analisis dinamis untuk sebuah file yang diselidiki akan diaktifkan dalam sebuah ruang lingkup yang aman baik pada sebuah mesin fisik yang telah disediakan sebagai virtual mesin untuk malware, selanjutnya mencari informasi mengenai effek komputer yang terjangkit file malware yang sedang diproses. Tahapan analisis dinamis ini akan memeriksa komputer dengan keseluruhan.

IV. Sistem Android

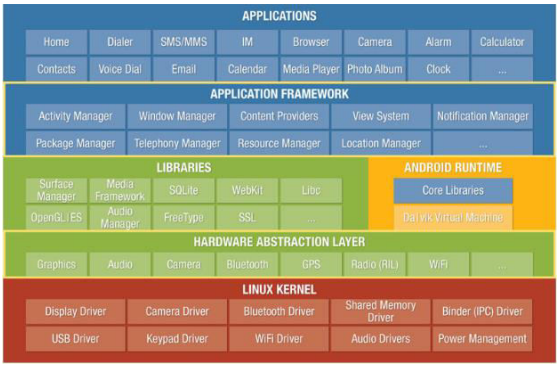
Android meruapakan sistem operasi yang berbasis linux untuk *handphone* seluler seperti *smarphone* dan tablet. Sistem android menyediakan fasilitas open souce bagi para pengembang untuk menciptakan aplikasi mereka sendri untuk digunakan oleh bermacam perangkat *handphone* [12]. Pada awalnya, google inc membeli android inc yang pendatang baru dalam membuat perangkat lunak untuk seluler. Untuk mengembangkan

 e-ISSN: 2615-8442

android dibutuhkan *Open Handset Alliance* dari 34 organisasi hardware, software, dan telekomunikasi seperti Google, HTC, Intel, Motorola, Qualcom, T-Mobile dan NVIDIA.

Pada awalnya pencuran android pada tahun 2007, android bersama organisasi *Open Handset Alliance* mendukung pengembangan dasar *open source* pada perangkat mobile. Di era sekarang terdapat dua jenis distributor sistem operasi android. Pertama yang mendapatkan dukungan penuh dari *Google Mail Services* (GMS) dan selanjutnya yang benar-benar bebas distribusinya tanpa dukungan langsung dari google yaitu *Open Handset Distribution* (OHD).

Terdapat 6 arsitektur grafis yang dimiliki sitem android , tampak gambar dibawah ini [1],[13] :

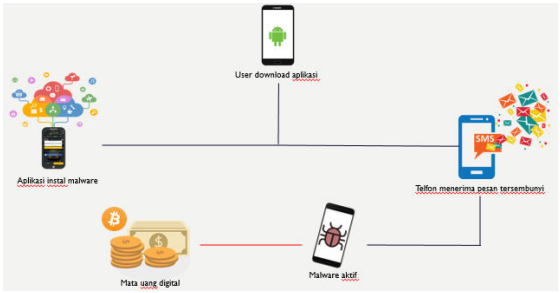


Gambar 3. Arsitektur Sistem Android

1. *Applications*
   Lapisan yang berisi aplikasi yang dikembangkan oleh pengembang android dan mempunyai aplikasi standar seperti browser dan SMS Client tetapi pengguna dapat membeli dan menginstal aplikasi baru ke *Application Layer*.
2. *Application Framework*
   Lapisan kedua untuk berkomunikasi langsung dengan Application Framework, dan cukup banyak penyediakan *tools* yang dibutuhkan untuk melakukan tujuan yang akan dirancang. Application Framework membangun fungsi dari aplikasi yang mereka buat. Selain aplikasi yang sebenarnya pada perangkat *Application Framework* juga berkomunikasi dengan lapisan *Libraries*.
3. *Libraries*
   Yang berfungsi untuk memproses berbagai jenis data, tetapi beberapa *lib* khusus untuk jenis perangkat tertentu.
4. *Android Runtime*
   Terdiri dari dua bagian besar yaitu Core lib dan *Dalvik Virtual Machine*. Core lib bertujuan untuk membuat dan menyebarkan kode dalam bahasa program java sedangkan *Dalvik Virtual Machine* seperti mesin mandiri dan mengeksekusi kode yang dibuat dengan Java Core Lib bertujuan sebagai perantara *Java Core Lib* dan *Hardware Abstraction Layer*.
5. *Hardware Abstraction Layer*
   Yang berkaitan dengan arsitektur Linux *Kernel*. Untuk menangani komunikasi antara hardware yang ditampilkan pada Linux *Kernel* dan semua lapisan *software* lain.
6. *Linux Kernel*
   Sistem operasi android pada dasarnya dibangun oleh Linux Kernel 2.6 dan juga menyediakan driver yang dibutuhkan perangkat linux untuk berkomunikasi dangan *Hardware Abstraction* Layer. Kernel juga menangani semua fungsi sistem operasi dasar perangkat android, contohnya alokasi memori, komunikasi jaringan, dan keamanan aplikasi.

V. Pembahasan

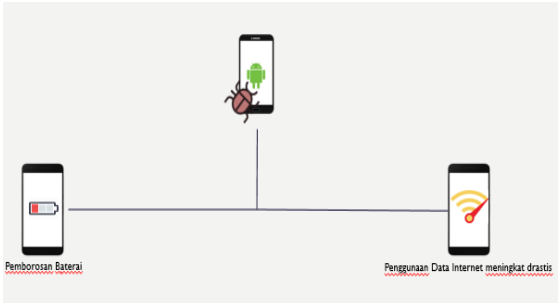
Berikut adalah ilustration kasus instal aplikasi yang terinfeksi malware :



Gambar 4. Ilustration Instal App Malware

Pada saat user men-*download* aplikasi dan menginstal aplikasi tersebut yang terinfeksi malware, maka telefon user tanpa sadar menerima pesan tersembunyi yang diakibatkan oleh malware tersebut dan perlahan malware bekerja dalam seluler user untuk mencari informasi mata uang digital.

Ilustrasi sederhana ciri-ciri android yang terkena malware :



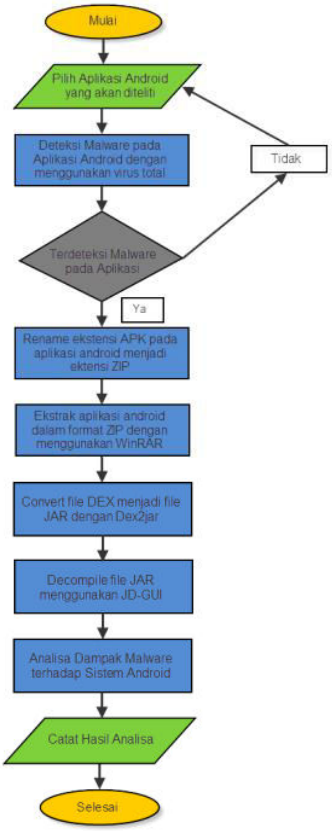
Gambar 5. Ciri-ciri android infeksi malware

Ketika smartphone kita terinfeksi malware tanpa disadari seluler mendapatkan kerusakan pada

 e-ISSN: 2615-8442

baterai menjadi boros dan penggunaan data internet meningkat signifikan akibat malware.

Berikut adalah flowchart metode analisa malware pada android :



Gambar 5. Flowchart Metode Analisa Malware

Bisa dilihat alur metode untuk menganalisa malware pada android. Hal pertama yang dilakukan adalah memilih aplikasi android yang akan diteliti, dalam hal ini aplikasi men-*download* dari forum contangio mobile. Aplikasi android yang terdapat mengandung malware android akan dianalisis dengan cara teknik analisis static. Aplikasi android yang terjangkit malware android dengan tipe file (.APK) direname menjadi tipe data (.ZIP), dan kemudian diekstrak dnegan menggunakan WinRaR, dikarenakan file APK dapat di ilustrasikan sebagai sebuah *archive* (ZIP) yang mengandung tipe file DEX, hasil dari ekstraksi berisikan beberapa file, terdapatlah file berektensi DEX. Selanjutnya file DEX diconvert ke format tipe data JAR dengan menggunakan tools Dex2jar dan akan mengeluarkan file tipe JAR.

Untuk langkah terakhir, file JAR di decompile menggunakan tools JD-GUI sehingga dapat dilihat semua *source code java* yang akan dianalisa untuk tujuan penelitian diharapkan mendeteksi malware pada android.

Penelitian ini akan bertuju kepada aplikasi android yang terjangkit malware yaitu *iCalender* (kuis.com).

VI. Analisis Malware pada *iCalender*

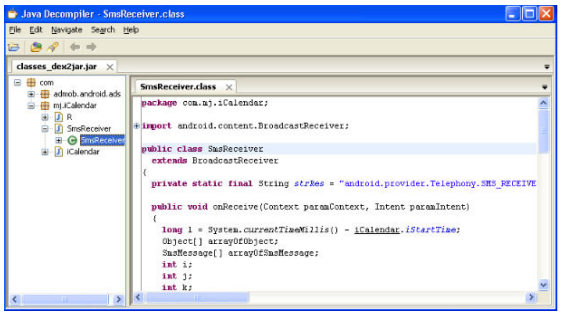
Aplikasi *iCalender* berfungsi sebagai kalender elektronik dan memiliki fitur tambahan yang disisipkan suatu malware.

Dari hasil analisa menggunkan layanan virus terdeteksi bahwa terdapat malware pada aplikasi *iCalender*.apk dan juga terdapat keanehan pada beberapa required permissions.

Gambar 6. *Detail required file iCalender*

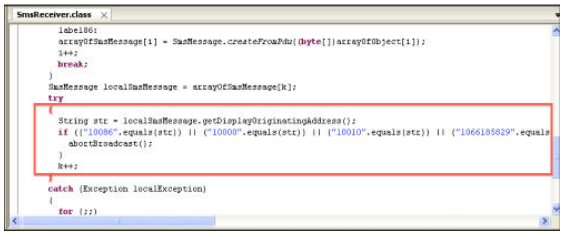
Peneliti melakukan analisis menggunakan tools komputer forensik. Di awali melakukan *rename* ekstensi APK menjadi ekstensi ZIP. Selanjutnya WinRAR dan akan menampilkan keluaran file bereksten DEX.

Langkah terakhir yaitu decompile file JAR dengan menggunakan tools JD-GUI sehingga menampilkan *output source code java* dari *iCalender*.apk.



Gambar 7. File *SmsReceiver*.class

Setelah dianalisis *source code smsreceiver* terdapat local SMS dengan address dan nomor mencurigakan (Gambar 8). Terdapat perintah abort broadcast berfungsi sebagai agar menolak laporan penerimaan SMS ke *smartphone*, sehingga user tanpa sadar ada aktifitas SMS yang berjalan.



Gambar 8. Analisa *Smsreceiver*

 e-ISSN: 2615-8442

Setelah dianalisa menggunakan search *engine* google, ternyata nomor "106618582" adalah layanan *service* provider dari operator China (Gambar 9).

Gambar 9. Mobile service provider China

Dari analisa di atas dapat merangkum kinerja malware yang terjangkit aplikasi iCalender.apk. malware tersebut aktif dan mengirimkan sms ke premium number 10668582 dengan isi SMS 921x1. Selanjutnya penjelasan di atas adanya penolakan laporan pengiriman dan penerimaan SMS dari premium number 10668582. Sehingga user tidak sadar aktifitas SMS yang bisa mengurangi saldo provider user gunakan.

Gambar 10. Informasi *iCalender*.apk

VII. Daftar Pustaka

1. A. HOOG., 2011. "Android Forenscs: Invesigation, Analysis and mobile Security for Google". Syngress.
2. ALMARRI, S., SANT, P., 2014. Optimised Malware Detection in Digital Forensics. IJNSA, Vol 6 (1).
3. CAHYANTO, T, A., WAHANGGARA, V., RAMADANA, D., 2017. Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis. JUSTINDO, Vol 3 (1).
4. FEIZOLLAH, ALI., etc., 2016. AndroDialysis : Analysis of Android Intent Effectiveness in Malware Detection. University of London, November 2016.
5. HAPTON, NIKOLAI,. BAIG, Z,. ZEADALLY, S., 2018. Ransomware behaviural analysis on windows platforms, JISA, pp 44-51.
6. ID CERT.net., 2018. Laporan Dwi Bulan I 2018 dari https://cert.or.id/bahan-bacaan/id/konten/31/ [diakses 19 July 2018]
7. KABAKUS, A, T., DOGRU, I, A., 2018. An in-depth analysis of Android malware using hybrid techniques. Digital Investigation, pp 1-9.
8. MASOOD, S. G., 2004. Malware Analysis for Administrators. Dari http://www.securityfocus.com/infocus/180 [diakses 1 Agustus, 2018]
9. SHIJO, P, V., SALIM, A., 2015. Integrated static and dynamic analysis for malware detection. ICICT. pp 804-811.
10. STATISTA., 2018, Market share held by the leading computer operating systems in the united states, dari https://www.statista.com/statistics/268237/global-market-share-held-by-operating-systems-since-2009/ [diakses 19 July 2018]
11. Statcounter Global Stats., 2018. Mobile Operating System Market Share in Indonesia from 2013 to 2017 dari http://gs.statcounter.com/os-market-share/mobile/indonesia [diakses 20 July 2018]
12. K.SHARMA, T., DAND, T. OH, W. STACKPOLE., 2013. "Malware Analysis for Android Operationg". 8th Annual Symposium on Information assurance, pp. 31-35, June 4-5
13. V. MANJUNATH., 2011. "Reverse Engineering Of Malware On Android, "in SANS Institute InfoSec Reading Room, University of Essex.