IMPLEMENTATION OF MALWARE DETECTION SERVICE ON ANDROID

Muhammad Habibi[1], Setia Juli Ismail[2], Anang Sularsa[3]

[1]Universitas Telkom, [2]Universitas Telkom, [3]Universitas Telkom

[1]mhdhabibi1294@gmail.com, [2]*jul@tass.telkomuniversity.ac.id*,

[3]*anang@tass.telkomuniversity.ac.id*

Abstrak

CProyek Akhir ini membuat aplikasi pendeteksi Malware android yaitu Andro Scanner. Saat ini android telah menjadi salah satu sistem operasi yang popular. Kesuksesan ini didukung dengan banyak aplikasi yang tersedia dan perkembangan ini diikuti dengan semakin banyaknya malware yang dibuat untuk android. Saat ini malware untuk Android semakin banyak, Majalah ICT mengatakan Android menjadi sasaran empuk dari Malware. Hal itu terungkap dari laporan terbaru perusahaan security online Kaspersky Lab, 99, 9% malware dalam perangkat smartphone yang terdeteksi pada paruh pertama tahun 2013 didesain untuk menyerang ponsel Android. Selain itu ada juga kebiasaan orang Indonesia yang tidak menginstalasi aplikasi dari google market resmi karena alasan berbayar, ataupun karena alasan koneksi yang lambat. Umumnya orang mengunduh file apk dari berbagai sumber, padahal banyak sekali file apk ini yang sudah disisipi malware. Andro Scanner adalah salah satu aplikasi yang dapat digunakan untuk melakukan deteksi malware pada file yang berekstensi Apk, fungsinya untuk mengetahui apabila file Apk tersebut terinfeksi malware.

Kata Kunci: AndroScanner, Android, Malware *Abstract*

This final project meant to build an Andro scanner application of detection Malware. Theseday, android platform have been one of the most popular operating system. One of the reason behind the success of android platform is their android market that provide the user with lots of application. The growth of android platform also followed by the malware that created to attack this operating system. Untill this time, the are tons of malware that can attack android. The ICT magazine says that android is really vulnerable target for malware. Kaspesky reveal that 99.9% detected on the mobile gadget from the first half of 2013 were designed to attack android phone, the Indonesian behavior of installing an app from unsecured source because of it is paid system makes the risk even worst. These application from unsecured source usually already injected with mallware. Andro scanner is one of scanner application that android user can use to detect malware from apk type of file, The purpose of this application is to detect wether the file is infected or not.

Keywords: Andro Scanner, Android, Malwre

1. Pendahuluan

1.1 Latar Belakang

Saat ini android telah menjadi salah satu sistem operasi yang popular. Kesuksesan android didukung dengan banyak aplikasi yang tersedia untuk android. Sayangnya perkembangan ini diikuti dengan semakin banyaknya malware yang dibuat untuk android, Majalah ICT mengatakan Android menjadi sasaran empuk dari Malware. Hal itu terungkap dari laporan terbaru perusahaan *security online* Kaspersky Lab, 99,9% *malware* dalam perangkat *mobile* yang terdeteksi pada paruh pertama tahun 2013 didesain untuk menyerang ponsel Android. Ada pula yang membuat Malware semakin menyebar yaitu kebiasaan orang Indonesia yang tidak menginstalasi aplikasi dari google market resmi karena alasan berbayar

Andro Scanner adalah salah satu aplikasi yang dapat digunakan untuk melakukan scanning malware pada file yang berekstensi Apk, fungsinya untuk mengetahui apabila file Apk tersebut terinfeksi malware. Aplikasi Androscanner untuk saat ini hanya dapat diakses melalui web browser. Tetapi cara ini kurang efektif karena cara ini memerlukan waktu lebih banyak. Pada proyek akhir ini dikembangkan berupa layanan deteksi malware pada Android. Layanan ini merupakan pengembangan dari Androscanner berbasis web yang sebelumnya pernah dibuat oleh mahasiswa D3 teknik komputer angkatan 2011, pada pengembangan layanan ini sduah dapat digunakan pada perangkat android. Pembangunan layanan ini menggunakan bahasa pemrograman Java dengan Android Studio. Pengujian dilakukan pada perangkat smartphone android dengan OS Marshmallow.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan maka dapat dirumuskan masalah, yaitu :

1. Bagaimana melakukan identifikasi pada apk yang terinfeksi Malware?
2. Bagaimana melakukan pengujian detektsi Malware pada layanan tersebut?

1.3 Tujuan

Berdasarkan rumusan masalah dan latar yang telah diuraikan, berikut tujuannya :

1. Membuat layanan deteksi malware berbasis Android

1.4 Definisi Operasional

Adapun definisi operasional pada proyek akhir ini ialah sebagai berikut :

1. Deteksi Malware

   Malware adalah (singkatan dari istilah Bahasa inggris malicious software, yang berarti perangkat lunak yang jahat) adalah program komputer yang diciptakan dengan maksud dan tujuan tertentu dari penciptanya dan merupakan program yang mencari kelemahan dari sebuah software. Umumnya malware diciptakan untuk membobol atau merusak suatu software atau operating system melalui script yang disisipkan secara tersembunyi oleh pembuatnya.

2. Android

   Android adalah OS (Operating System) merupakan sistem operasi berbasis linux untuk telepon selular, komputer tablet dan Android menyediakan platform terbuka untuk para pengembang agar dapat menciptakan aplikasi mereka sendiri. Pada awalnya Android dikembangkan oleh Android Inc itu sendiri dengan dukungan finansial dari Google, yang kemudian membelinya pada tahun 2005.

   Kesimpulanya adalah Aplikasi Androscanner yang di buat di Android berhasil dilakukan dan aplikasi dapat melakukan pemindaian Malware terhadap file yang berekstensi apk.

1.5 Metode Pengerjaan

Metode yang digunakan adalah sebagai berikut :

1. Studi Literatur

   Mempelajari hal yang berkaitan dengan proyek akhir, seperti Java, Android Studio, Android dan lain-lain.

2. Analisis Kebutuhan Sistem

   Langkah ini diperlukan untuk mengetahui kebutuhan hardawre dan software yang akan digunakan, mempersiapkan perangkat komputer serta peralatan lain yang mendukung proyek akhir.

3. Implementasi

   Langkah selanjutnya adalah implementasi termasuk juga kegiatan instalasi dan konfigurasi semua layanan yang dibutuhkan.

4. Pengujian

   Pengujian dilakukan setelah instalasi dengan konfigurasi berjalan dengan baik, berupa pengecekan terhadap aplikasi yang sudah dibuat berbasis Android.

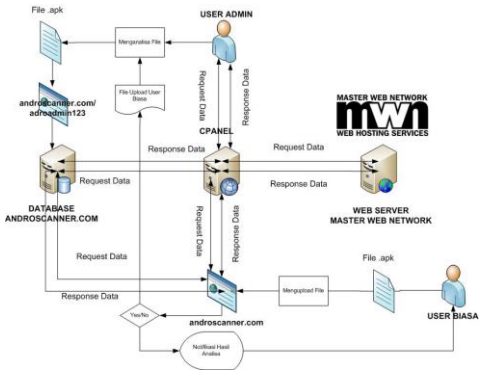
5. Penyusunan Laporan

   Pada langkah ini semua metode yang telah dilakukan akan dibuat dokumentasinya.

2. Tinjauan Pustaka

2.1 AndroScanner

Pada gambar 2.1 merupakan struktur sistem aplikasi Androscanner yang akan dibangun. Terdapat 4 komponen utama yaitu Web server dari PT. Master Web Network, Database Website Androscanner, Halaman CPANEL Website, Halaman Website Androscanner. Dan terdapat 2 sisi User yaitu user biasa yang mengakses halaman user dan user yang menjadi admin untuk mengakses halaman administrator. Webserver dari PT. Master Web Network berfungsi sebagai penyedia layanan DNS dan Web Hosting dengan aplikasi CPANEL. Database Website Androscanner.com berfungsi untuk menyimpan data yang diinputkan oleh user admin dan menyimpan data file yang di upload oleh user. Halaman CPANEL digunakan untuk mengelola file resource pada website. Halaman Website menyediakan tampilan untuk user biasa dan user admin sebagai media yang digunakan pada aplikasi Androscanner.



Gambar 1 Struktur AndroScanner

2.2 Android

Pada gambar 2 ini adalah sruktur dari Android

1. Layer Applications dan Widget

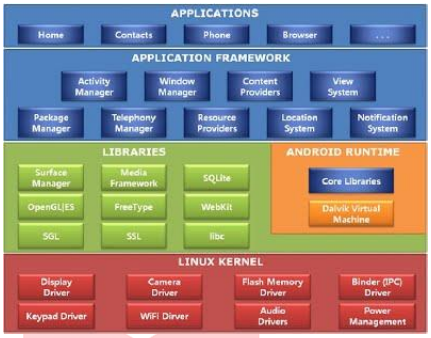
   Inilah layer pertama pada OS Android, biasa dinamakan layer Applications danWidget. Layer ini merupakan layer yang berhubungan dengan aplikasi-aplikasi inti yang berjalan pada Android OS. Seperti klien email, program SMS, kalender, browser, peta, kontak, dan lain-lain. Semua aplikasi ini dibuat dengan menggunakan bahasa Java. Apabila kalian membuat aplikasi, maka aplikasi itu ada di layer ini.

2. Layer Applications Framework

   Applications Framework merupakan layer dimana para pembuat aplikasi menggunakan komponen-komponen yang ada di sini untuk membuat aplikasi tersebut. Kerangka aplikasi menyediakan kelas-kelas yang dapat digunakan untuk

3. Layer Libraries

Libraries merupakan layer tempat fitur-fitu rAndroid berada. Pada umumnya libraries diakses untuk menjalankan aplikasi. Android menggunakan beberapa paket pustakayang terdapat pada C/C++ dengan standar Berkeley Software Distribution (BSD)hanya setengah dari yang aslinya untk tertanam pada kernel Linux.Beberapa pustaka diantaranya:



Gambar 2 Struktur Android [11]

2.3 Java

Java merupakan bahasa pemrograman berorientasi objek yang dikembangkan oleh Sun Microsystem, suatu perusahaan yang terkenal dengan Workstation UNIX high-end.Sejak dirilis pada tahun 1995, bahasa pemrograman Java dengan cepat memperoleh popularitas di kalangan para pemrogram. Keberhasilan ini disebabkan teknologi baru yang diperkenalkan Sun Microsystems yaitu Java Virtual Machine (JVM), yang memungkinkan sebuah aplikasi dijalankan di atas platform apa saja sepanjang pada mesin tersebut dipasang JVM. Program yang dihasilkan dengan bahasa Java dapat berupa applet (aplikasi kecil yang berjalan di atas web browser) maupun berupa aplikasi mandiri yang dijalankan dengan program Java Interpreter.

- kelebihan

a. Multiplatform.

Kelebihan utama dari Java ialah dapat dijalankan di beberapa platform / sistem operasi komputer, sesuai dengan prinsip tulis sekali, jalankan di mana saja.

- Kekurangan

a. Tulis sekali

jalankan di mana saja - Masih ada beberapa hal yang tidak kompatibel antara platform satu dengan platform lain

2.4 Malware

Malware adalah istilah yang digunakan untuk perangkat lunak berbahaya yang dirancang untuk merusak atau melakukan tindakan yang tidak diinginkan terhadap sistem komputer.
Jenis-jenis malware ini diantaranya adalah trojan, virus, worm, spyware, adware, rootkit dan sebagainya. Berikut beberapa pengertian dari jenis-jenis malware :

- Virus Komputer adalah jenis malware yang menyerang file eksekusi (.exe) yang akan menyerang dan menggandakan diri ketika file exe yang terinfeksi di jalankan. Virus komputer menyebar dengan cara menyisipkan program dirinya pada program atau dokumen yang ada dalam komputer
- Worm adalah sebuah program komputer yang dapat menggandakan dirinya secara sendiri dalam sistem komputer. Sebuah worm dapat menggandakan dirinya dengan memanfaatkan jaringan (LAN/WAN/Internet) tanpa perlu campur tangan dari user itu sendiri.Worm memanfaatkan celah keamanaan yang memang terbuka atau lebih dikenal dengan sebutan vulnerability.
- Spyware adalah program yang bertindak sebagai mata-mata untuk mengetahui kebiasaan pengguna komputer dan mengirimkan informasi tersebut ke pihak lain. Spyware biasanya digunakan oleh pihak pemasang iklan.
- worm-rootkit-trojan-keylogger

Trojan atau trojan hourse adalah program yang diam-diam masuk ke komputer kita, kemudian memfasilitasi program lain misalnya virus, sypware, adware. keylogger dan malware lainnya untuk masuk, merusak sytem, memungkinkan orang lain meremote komputer dan mencuri informasi seperti password atau nomor kartu kredit kita

3. Analisis Dan Perancangan

3.1 Analisis Kebutuhan Sistem

3.1.1 Kebutuhan Perangkat Keras

Adapun spesifikasi minimum yang dipakai adalah sebagai berikut :

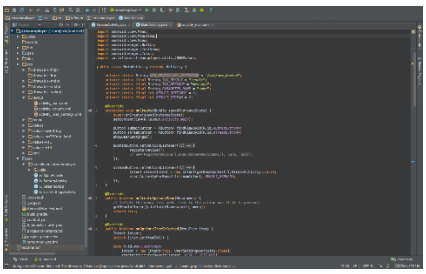
1. Laptop
   Spesifikasi :
   a. Processor : Intel Core i3
   b. Ram : 4 GB
   c. Harddisk : 500GB
   d. Operating System : Windows 7 Ultimate 64-bit

2. Smartphone
   Spesifikasi
   a. Ram : 2 Gb
   b. Processor : Quadcore 1,5Ghz
   c. Memory internal : 16 Gb
   d. Os : Marshmallow

3.1.2 Kebutuhan Perangkat Lunak

Adapun kebutuhan perangkat lunak yang dibutuhkan adalah sebagai berikut :

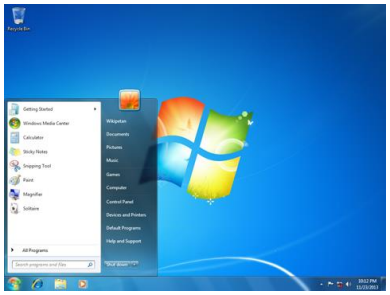
1. Android Studio



Gambar 3 Tampilan Awal Android Studio

Pada Gambar 3 merupakan tampilan awal aplikasi Android Studio, perangkat lunak ini digunakan untuk pemrograman sistem dan pembangunan aplikasi android. *Software* ini diinstal di laptop

2. OS Windows 7



Gambar 4 Dekstop Windows 7

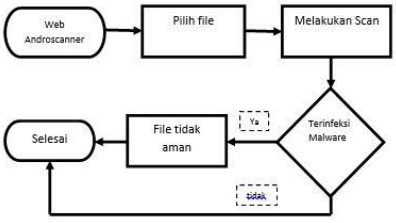
Pada Gambar 4 merupakan tampilan desktop Windows 7 pada laptop.

3. Os Marshmallow

Gambar 5 Os Marshmallow

Pada Gambar 5 merupakan tampilan yang menunjukan smartphone menggunakan Os marshmallow.

3.2 Perancangan Sistem



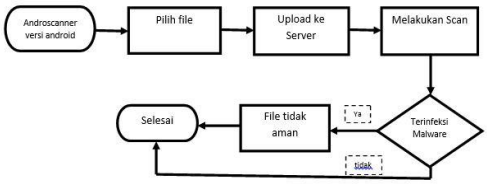
Gambar 6 Perancangan Sistem Androscannerberbasis Web

Pada Gambar 6 merupakan perancangan sistem yang terdapat pada Web Androscanner

1. Dibagina pilih file, pengguna dapat memilih file yang ada pada storage
2. Dibagian melakukan scan, file yang sudah dipilih dilakukan pemindaian Malware

3. Dibagian terinfeksi Malware, sudah mendapatkan hasil dari pemindaian apabila file terinfeksi Malware atau ama dari Malawre

Dibagian perancangan sistem pada Androscanner berbasis Android



Gambar 7 Perancangan Sistem Androscanner berbasis Android

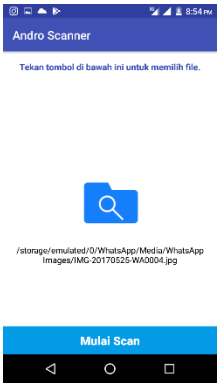
1. Dibagian pilih file, pengguna memilih file yang akan dilakukan pemindaian
2. Dibagian upload ke server, file yang sudah dipilih diupload ke server untuk dilakukan pemindaian
3. Dibagian melakukan scan, file yang sudah dipilih dilakukan pemindaian Malware
4. Dibagian terinfeksi Malware, sudah mendapatkan hasil dari pemindaian apabila file terinfeksi Malware atau ama dari Malawre

4. Implementasi dan Pengujian

4.1 Implementasi

4.1.1 Melakukan pemindaian dari Android

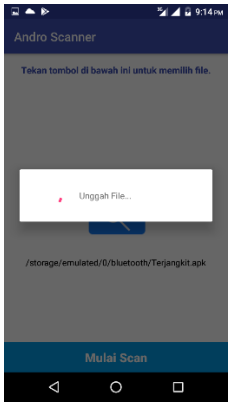
a. Proses pemilihan file



Gambar 8 proses pemilihan file

Pada Gambar 8 merupakan proses pemilhan file yang terdapat pada Android

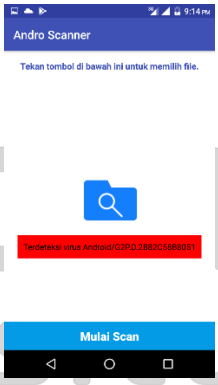
b. Proses unggah



Gambar 9 proses pengunggahan

Pada gambar 9 merupakan proses pengunggahan file ke server

c. Hasil pemindaian terinfeksi Malware



Gambar 9 proses pengunggahan

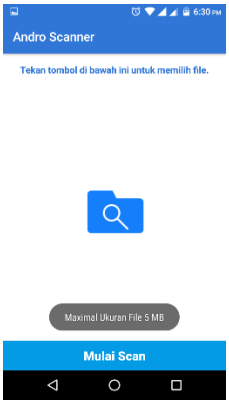
Pada gambar 9 ini adalah hasil dari pemindaian file dan hasilnya file terinfeksi Malawre

d. File aman dari Malware

Gambar 10 proses pengunggahan

Pada gambar 10 ini adalah hasil dari pemindaian file dan hasilnya file aman dari Malware

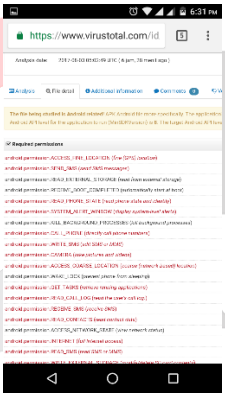
e. Fitur pembatasan ukuran file



Gambar 11 pembatasan file

Pada gambar 11 yaitu fitue untuk membatasi file yang akan dilakukan pemindaian agar aplikasi ini dapat bekerja dengan baik

f. Fitur melihat detai



Gambar 12 melihat detail hasil pemindaian

Pada gambar 12 yaitu melihat detail dari hasil pemindaian

4.2 Pengujian

4.2.1 pengujian 20 apk yang menggunakan metode AVG

Pada pengujian ini dilakukan pada 20 file apk menggunakan metode pemindaian AVG

Tabel 1 pengujian menggunakan metode AVG

	Hasil	
Nama File	Terinfeksi Malware	Tidak Terinfeksi Malware
com.fdhgkjhtkjbx.apk	-	ya
com.parental.contr.v4.dexguard.ap	ya	-
com.parentcontrol.v5.apk	ya	-
Descandra.apk	ya	-
Org.banews.apk	ya	-
masnu.apk	ya	-
smsThief.apk	ya	-
smsWorker.apk	ya	-
terinfeksi_Malware.apk	ya	-
apk APP_lock_v2_30.3.apk	tidak	-
Busybox_v50.apk	tidak	-
com.fab.md5.apk	tidak	-
disk_digger_photo.apk	tidak	-
eProxy_v2.apk	tidak	-
Hack_app_v1.apk	tidak	-
HashDroid_v3.3.apk	tidak	-
Real Followers.apk	tidak	-
googleplay.apk	tidak	-
SB Tool Game.apk	tidak	-

Kesimpulan yang didapat dari hasil pengujian bahwa:

a. dari 10 apk terinfeksi Malware ada 1 apk yang didapati bebas dari Malware

b. dari 10 apk bebas Malware semua apk aman dari terinfeksinya Malware

4.2.2 pengujian 20 apk yang menggunakan metode KASPERSKY

Pada pengujian ini dilakukan pada 20 file apk menggunakan metode pemindaian KASPERSKY

Tabel 2 pengujian menggunakan metode KASPERSKY

	Hasil	
Nama File	Terinfeksi Malware	Tidak Terinfeksi Malware
com.fdhgkjhtkjbx.apk	ya	-
com.parental.contr.v4.dexguard.ap	ya	-
com.parentcontrol.v5.apk	ya	-
Descandra.apk	ya	-
Org.banews.apk	ya	-
masnu.apk	ya	-
smsThief.apk	ya	-
smsWorker.apk	ya	-
terinfeksi Malware.apk	ya	-
apk APP_lock_v2_30.3.apk	tidak	-
Busybox_v50.apk	tidak	-
com.fab.md5.apk	tidak	-
disk_digger_photo.apk	tidak	-
eProxy_v2.apk	tidak	-
Hack_app_v1.apk	tidak	-
HashDroid_v3.3.apk	tidak	-
Real Followers.apk	tidak	-
googleplay.apk	tidak	-
SB Tool Game.apk	-	ya

Kesimpulan yang didapat dari hasil pengujian bahwa:

a. dari 10 apk terinfeksi Malware semua berhasil di pindai dan terinfeksi Malware

b. dari 10 apk bebas Malware ada 1 apk yang didapati terinfeksi dari Malware

5. Penutup

5.1 Kesimpulan

Berdasarkan dari hasil proses implementasi dan pengujian yang dilakukan pada Proyek Akhir ini, maka dapat diambil beberapa kesimpulan sebagai berikut :

1. Androscanner berbasis Android berhasil dibangun dan berhasil memindai file
2. Androscanner berhasil mendeteksi Malware.

5.2 Saran

Berdasarkan dari hasil implementasi Proyek Akhir ini terdapat beberapa saran yang diambil yaitu sebagai berikut :

a. Tugas akhir ini dapat ditingkatkan dengan server buatan sendiri dan di tambahkan database

b. Pengujian file bisa dilakukan di Os Kitkas, Nougat, dan pada perangkat tablet

Daftar Pustaka

[1] W. KOMPUTER, Android Programming, Yogyakarta: ANDI DAN WAHANA KOMPUTER, 2013.

[2] S. J. I. Ismail, "Androscanner," 13 Agust 2014. [Online]. Available: http://julismail.staff.telkomuniversity.ac.id/androscanner-malware-scanner-android/. [Accessed 24 mei 2015].

[3] ashishb, "Sample Malware," 18 January 2016. [Online]. Available: https://github.com/ashishb/android-malware. [Accessed 24 Mei 2017].

[4] Androiddhive, "ANDROID Json Parsing Tutorial," 5 January 2014. [Online]. Available: http://www.androidhive.info/2012/01/android-json-parsing-tutorial/. [Accessed 9 July 2016].

[5] A. Barber, "Stack Over Flow file chooser," 12 July 2013. [Online]. Available: https://stackoverflow.com/questions/7856959/android-file-chooser. [Accessed 2 December 2015].

[6] Dan, "Android L likely to mean Lemon," 23 August 2014. [Online]. Available:

http://www.androidguys.com. [Accessed 9 January 2016].

[7] ignite.apache.org, "Powered by Java," [Online]. Available: https://ignite.apache.org/features/java.html. [Accessed 5 January 105].

[8] http://4.bp.blogspot.com, "Malware," [Online]. Available: http://4.bp.blogspot.com.

[9] Virustotal.com, "Virustotal.com," [Online]. Available: Virustotal.com.

[10] http://www.majalahict.com/, "Android ternyata jadi sasaran empuk malware," 20 Juni 2014. [Online]. Available: http://www.majalahict.com/android-ternyata-jadi-sasaran-empuk-malware/. [Accessed 20 mei 2017].

[11] J. ZAELANI, "https://sites.google.com/a/student.unsika.ac.id/bongkar-os-linux/struktur-sistem-operasi/struktur-sistem-operasi-android," 9 Agus 2014. [Online]. Available: https://sites.google.com/a/student.unsika.ac.id/bongkar-os-linux/struktur-sistem-operasi/struktur-sistem-operasi-android. [Accessed 20 july 2017].

[12] www.oracle.com, "http://www.oracle.com/technetwork/java/index.html," ORACLE, 12 July 2014. [Online]. Available: http://www.oracle.com/technetwork/java/index.html. [Accessed 18 July 2017].

[13] http://www.catatanteknisi.com, "Catatan Tekniksi," Catatan Tekniksi, 20 May 2014. [Online]. Available: http://www.catatanteknisi.com/2011/12/pengertian-jenis-jenis-malware.html. [Accessed 18 July 2017].

[14] T. R. K. 6302110152, "Androscanner," *IMPLEMENTASI DAN PENGUJIAN APLIKASI SCAN MALWARE BERBASIS WEB DENGAN KEAMANAN SSL DAN,* no. 3, p. 3, 2012.