CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 2, No. 1, Mei 2019, hlm. 24-29

KASUS KEJAHATAN SIBER PADA TELEPON SELULER ANDROID

Nova Setiawan
Program Studi Teknik Informatika, Fakultas Teknologi Industri UII
Email: dnoovas@gmail.com

Abstrak

Telepon seluler sudah menjadi bagian dari kehidupan sehari-hari yang dapat ditemukan di semua lapisan masyarakat. Telepon yang kini dikenal dengan istilah *smartphone* memiliki banyak fitur didalamnya untuk memudahkan pengguna melakukan berbagai transaksi. Mulai dengan transaksi komunikasi, transaksi data, dan transaksi penjualan dapat dilakukan oleh *smartphone* dengan mudah. Dibekali dengam sistem operasi *Android* yang di kembangkan oleh *Google* peruhaan raksasa dibidang teknologi informasi. Banyak sekali celah yang dapat dimanfaatkan untuk dilakukan tindak kejahatan pada telepon seluler tersebut atau yang dikenal dengan *Cybercrime* khususnya pada telepon seluler. *Malware* adalah telepon lunak ganas yang khusus dibuat untuk menyerang telepon seluler atau perangkat cerdas lainnya. Awalnya, *malware* hanya melihat sisi kerentanan keamanam system perangkat lunak, namun seiring dengan perkembangannya *malware* berubah secara bertahap dan dapat dimanfaatkan untuk mendapatkan keuntungan secara finansial. *Malware* yang ditujukan untuk *smartphone* sampai saat ini sudah mengalami perkembang dengan pesat yang mengancam keamanan system keamanan *android* untuk diserang

Kata kunci: *Cybercrime, malware, mobile hacking*

CASE OF CYBER CRIME ON MOBILE PHONE ANDROID

Abstract

Cell phones have become part of everyday life that can be found in all walks of life. Phones that are now known as smartphones have many features in them to make it easier for users to carry out various transactions. Starting with communication transactions, data transactions, and sales transactions can be done easily by smartphone. Equipped with the Android operating system that was developed by Google giant company in the field of information technology. There are so many loopholes that can be used to do crime on these cellular phones, or known as Cybercrime, especially on cellular phones. Malware is a malignant soft phone specifically designed to attack cellular phones or other intelligent devices. Initially, malware only saw the security vulnerability of the software system, but along with its development malware changed gradually and could be used to gain financial benefits. Malware intended for smartphones, to date has experienced rapid growth that threatens the security of the Android security system

Keywords*: Cybercrime, malware, mobile hacking*

1. PENDAHULUAN

Telepon seluler sudah menjadi bagian dari kehidupan sehari-hari yang dapat ditemukan di semua lapisan masyarakat. Telepon yang kini dikenal dengan istilah *smartphone* memiliki banyak fitur didalamnya untuk memudahkan pengguna melakukan berbagai transaksi. Mulai dengan transaksi komunikasi, transaksi data, dan transaksi penjualan dapat dilakukan oleh *smartphone* dengan mudah. Dibekali dengam sistem operasi *Android* yang di kembangkan oleh *Google* peruhaan raksasa dibidang teknologi informasi. Sampai saat ini *android* sudah mencapai versi O atau yang di kenalkan dengan nama *android oreo* memiliki keunggulan dari versi-versi seri sebelumnya.

Dengan kemudahan yang diberikan oleh telepon seluler *android* ini tidak menjamin transaksi yang dilakukan berjalan aman dan tidak ada masalah. Banyak sekali celah yang dapat dimanfaatkan untuk dilakukan tindak kejahatan pada telepon seluler tersebut atau yang dikenal dengan *Cybercrime* khususnya pada telepon seluler. Kejahatan siber yang menyerang telepon seluler dikelompokan menjadi 11 oleh Pavan DugaL yaitu 1.*Mobile Hacking, 2.Mobile Cyber Defamation, 3.Mobile Pornography, 4.Identity Theft, 5. Cloning or re-chapping of mobile, 6.Mobile Cyber Stalking, 7.Denial of service Attack, 8.Mobiles Virus Dissemination, 9.Mobile Software Piracy, 10.Mobile Credit Card Fraud, dan 11.Mobile Phishing.* Dari pengelompokan jenis-jenis kejahatan seluler tersebut dapat diketahui telepon seluler sangat rentan sekali mendapat serangan kejahatan tertentu tanpa disadari oleh pemilik perangakat tersebut.

Malware adalah telepon lunak ganas yang khusus dibuat untuk menyerang telepon seluler atau perangkat cerdas lainnya. Awalnya, *malware* hanya melihat sisi kerentanan keamanam system perangkat lunak, namun seiring dengan perkembangannya *malware* berubah secara bertahap dan dapat

dimanfaatkan untuk mendapatkan keuntungan secara finansial. *Malware* yang ditujukan untuk *smartphone* sampai saat ini sudah mengalami perkembang dengan pesat yang mengancam keamanan system keamanan *android* untuk diserang. Terdapat dua kategori *malware* dalam yang menajdi ancaman perangkat seluler adalah personal *spyware* dan *grayware. Spyware* dapat mengumpulkan informasi seperti lokasi, pesan SMS, dan riwayat panggilan tanpa diketahui oleh pemilik.

2. LANDASAN TEORI

2.1. Definisi Cybercrime

Agar dapat memudahkan pemahaman, berikut beberapa pendapat tentang apa itu *cybercrime.* Menurut Gregory (2009) *cybercrime* adalah suatu bentuk kejahatan vitual dengan memanfaatkan perangkat komputer atau perangkat seluler yang terhubung dengan internet, dan mengekploitasi telepon seluler lainya yang tehubung dengan internet. Adanya celah keamanan pada sistem operasi menyebabkan kelemahan dan terbukanya celah yang dapat digunakan para *hacker* untuk menyusup kedalam sistem perangkat seluler.

Cybercrime lebih dikenal dengan nama kejahatan dunia maya. *Cybercrime* merupakan salah satu bentuk kejahatan yang tidak boleh dilakukan oleh semua orang. *Cybercrime* adalah kejahatan yang dilakukan dalam dunia maya melalui komputer atau internet. *Cybercrime* termasuk dalam kategori tindakan kejahatan kriminal. *Cybercrime* telah banyak dilakukan oleh orang-orang yang tidak bertanggung jawab dalam menggunakan teknologi.

Cybercrime bisa dilakukan oleh orang yang menguasai bidang teknologi. *Cybercrime* bisa dilakukan dimana saja sesuai dengan keinginan pelaku. Pelaku *cybercrime* bisa disebut dengan *Hacker*. *Hacker* akan menyerang sistem komputer untuk melancarkan usahanya untuk melakukan kejahatan dalam dunia maya. *Hacker* bisa saja mencuri data pribadi anda, dan melakukan pembobolan kredit. Banyak jenis kejahatan *Cybercrime* yang bisa dilakukan oleh sang *Hacker*.

2.2. *Malware*

Malware merupakan perangkat lunak yang diciptakan untuk menyusup atau merusak sistem komputer. Istilah ini umum dipakai oleh pakar komputer untuk mengartikan berbagai macam perangkat lunak atau kode perangkat lunak yang mengganggu atau mengusik.

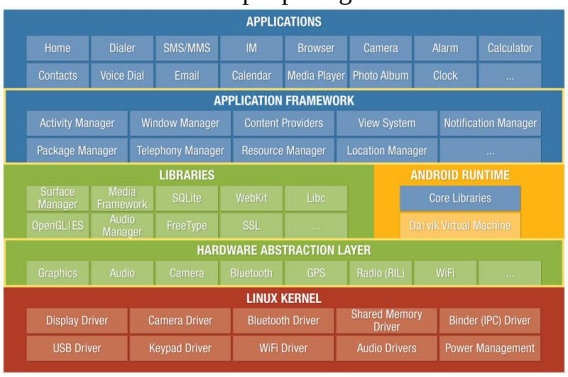
Perangkat lunak yang dianggap sebagai perangkat perusak berdasarkan maksud yang terlihat dari pencipta dan bukan berdasarkan ciri-ciri tertentu, mencakup *Virus Computer*, *Trojan Horse*, perangkat pengintai *spyware*), perangkat iklan (*adware*) yang tidak jujur, perangkat jahat (*crimeware*) dan perangkat lunak lainnya yang berniat jahat dan tidak diinginkan.

2.3. Android

Android merupakan sistem operasi yang berbasis *opensource* atau yang dikenal dengan *linux* untuk sistem pada perangkat seluler. *Android* dikembangkan langsung oleh Android Inc. dengan dukung penuh dari *Google Finance* namun kemudian dibeli pada tahun 2005. Setelah itu, Android resmi liris pada tanggal 5 November 2007 bersamaan dengan berdirinya *Open Handset Alliance* yang mana merapakan perusahaan telekomunikasi yang bertujuan untuk dapat memajukan standar dari perangkat seluler yang ada.

Di sisi lain, pihak Google merilis kode-kode pada Android di bawah naungan lisensi *Apache* yang mana merupakan lisensi perangkat lunak serta standar terbuka untuk perangkat seluler. Terdapat 2 jenis distributor resmi dari sistem *Android*, yang pertama memiliki dukungan penuh *Google* (*Google Mail Services*) dan yang kedua adalah distributor yang memang benar benar bebas tanpa adanya dukungan dari Google yang sering disebut *Open Handset Distribution (OHD)*. *Smartphone* yang pertama kali diluncurkan ke publik dengan menjalankan sistem *Android* yaitu HTC *Dream* yang diluncurkan pada tanggal 22 Oktober 2008. Nah kali ini akan dijelaskan lebih lanjut mengenai pengertian *Android* beserta hal-hal yang terkait di dalamnya.

Arsitektur grafis yang ada pada sistem operasi android dapat disebut "*architecture of Android"* contoh terdapat pada gambar berikut.



Gambar 1. Arsitektur Sistem Android

Applications

Lapisan atas dari arsitektur android yang berisi aplikasi yang dikembangkan oleh pengembang android. Ada beberapa aplikasi standar yang, seperti *Browser* atau *SMS client*, namun pengguna dapat membeli dan menginstal aplikasi baru ke a*pplication Layer*.

Application Framework

Application Framework adalah lapisan kedua dalam arsitektur android. Aplikasi berkomunikasi langsung dengan *Application Framework*, yang cukup banyak

menyediakan *tools* yang dibutuhkan untuk melakukan tujuan apa pun yang dirancang. Pengembang aplikasi langsung mengakses *Application Framework* untuk membangun fungsi dari aplikasi yang mereka buat. Selain aplikasi yang sebenarnya pada perangkat, *Application Framework* juga berkomunikasi dengan lapisan *Libraries* arsitektur android.

Libraries
Libraries asli android pada dasarnya hanya terdiri dari sejumlah fungsi yang memungkinkan perangkat untuk memproses berbagai jenis data. Beberapa *Libraries* ini khusus untuk jenis perangkat tertentu, serta dianggap *generic* untuk semua perangkat android.

Android Runtime
Android Runtime terdiri dari dua bagian besar, yaitu: *Core Libraries* dan *Dalvik Virtual Machine*. *Core Libraries* memungkinkan pengembang aplikasi android untuk membuat dan menyebarkan kode dalam Bahasa pemrograman java. *Libraries Core* ini akan memiliki akses ke *Libraries* asli android serta *Dalvik Virtual Machine*. *Dalvik Virtual Machine*, fungsi aplikasi ini seolah-olah mesin mandiri dan mengeksekusi kode yang dibuat dengan *Java Core Libraries*. Hal ini juga berfungsi sebagai perantara antara *Java Core Libraries* dan *Hardware Abstraction Layer* dari perangkat Android.

Hardware Abstraction Layer
Beberapa diagram arsitektur android memiliki HAL yang termasuk bagian dari Linux Kernel. HAL pada dasarnya menangani komunikasi antara perangkat keras yang ditampilkan pada Linux Kernel dan semua lapisan perangkat lunak lain.

Linux Kernel
Sistem operasi Android pada dasarnya dibangun di atas Linux kernel 2.6 dan menyediakan *driver* yang dibutuhkan perangkat Linux untuk berkomunikasidengan modul dari *Hardware Abstraction Layer*. Kernel Linux juga menangani semua fungsi sistem operasi dasar untuk perangkat android, seperti alokasi memori, komunikasi jaringan, dan keamanan aplikasi.

3. PEMBAHASAN

3.1. Jenis-jenis Kejahatan Seluler

Pengelompokan jenis kejahatan pada perangkat seluler dapat di kategorikan kedalam 11 jenis kejahatan yang sering terjadi pada perangkat seluler, berikut jenis-jenis kejahatan dalam perngkat selular

1.*Mobile Hacking*
Peretasan / gangguan ilegal yang masuk ke dalam sistem operasi seluler atau jaringan. Setiap tindakan yang dilakukan untuk membobol perangkat seluler, misalnya komunikasi, data dan jaringan. Peretas menggunakan program komputer siap pakai untuk menyerang komputer target, perangkat seluler atau alat komunikasi.

2.Mobile Cyber Defamation
Kejahatan semacam ini telah menjadi lazim di seluruh dunia saat ini. Penjahat mengirim SMS atau email yang merendahkan, menghina, dan tidak senonoh dengan menggunakan ponsel, perangkat seluler, dan perangkat komunikasi mereka, sehingga mencemarkan nama baik orang lain dan menurunkan reputasi mereka di mata orang-orang yang sangat menghargai mereka.

3.Mobile Pornography
Kejahatan yang memanfaatkan internet untuk digunakan oleh para pelaku menjangkau dan menyalahgunakan anak-anak dengan mengirimkan konten-konten dewasa yang berbau sex. Internet sangat cepat menjadi komoditas rumah tangga. Karena lebih banyak rumah memiliki akses ke internet, lebih banyak anak akan menggunakan ponsel, perangkat komunikasi, internet, dan lebih banyak lagi kemungkinan menjadi korban agresi pedofil.

4.Identity Theft
Perangkat selular digunakan untuk pencurian identitas dan setelah mendapatkan akan digunakan tindak kejahatan seperti penipuan berlangganan dll. Menggunakan berbagai perangkat komunikasi.

5. Cloning or re-chapping of mobile
Klon adalah ponsel analog yang telah diprogram untuk meniru identitas yang dimiliki oleh pelanggan yang sah dengan menggunakan ESN dan nomor telepon (nomor ini biasanya diperoleh dengan intersepsi dengan radio 'pemindai', pencurian catatan provider atau penyedia layanan atau langsung dari telepon yang ditirukan).

6.Mobile Cyber Stalking
Cyber Stalking dapat didefinisikan sebagai tindakan berulang pelecehan atau perilaku mengancam penjahat *cyber* terhadap korban dengan menggunakan layanan internet perangkat seluler. Menguntit dalam istilah umum dapat disebut sebagai tindakan pelecehan berulang yang menargetkan korban seperti mengikuti korban, membuat panggilan telepon melecehkan, membunuh hewan peliharaan korban, merusak properti korban, meninggalkan pesan tertulis atau benda.

7.Denial of service Attack
Ini adalah tindakan oleh penjahat, yang membanjiri bandwidth jaringan korban atau mengisi kotak e-

mailnya dengan email spam. Agar terjadi hang karena penggunaan memory yang berlebihan dan memberatkan system operasi sehingga perangkat menjadi hang atau mati.

8.Mobiles Virus Dissemination
Virus *malware android* menjadi salah satu terbesar yang sering terjadi adalah virus elektronik yang menargetkan perangkat selular atau perangkat komunikasi lainnya. Dalam perangkat lunak penyebaran virus yang khas, perangkat lunak berbahaya melekatkan dirinya ke perangkat lunak lain.

9.Mobile Software Piracy
Pencurian perangkat lunak seluler melalui penyalinan ilegal program asli atau pemalsuan dan distribusi produk yang dimaksudkan untuk mendapatkan seperti yang asli untuk yang asli. Tren yang saat ini adalah melukuan pelanggaran hak cipta aplikasi.

10.Mobile Credit Card Fraud
Penggunaan kartu kredit yang tidak sah dan ilegal melalui perangkat selular untuk membeli produk atau layanan.

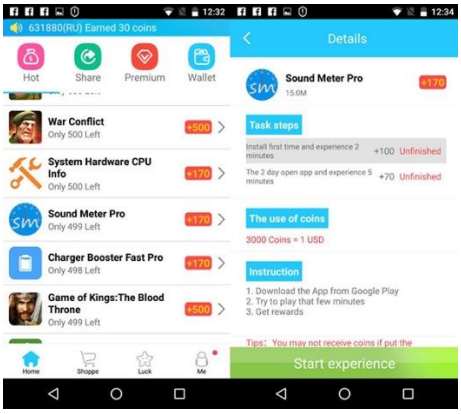
11.Mobile Phishing.
Ini lebih mengarah pada tindakan yang menargetkan pengguna perangkat selular dengan *phishing email* atau mengirimkan email palsu yang tampaknya berasal dari penyedia layanan seluler yang asli.

3.2. Contoh Kasus

Malware ini menjadikan perangkat *mobile* sebagai target. Namun demikian terdapat indikasi serangan ini dapat juga diimplementasikan pada perangkat lain. *Malware* ini menginfeksi perangkat dengan berbagai modus. Salah satunya *malware* ini meduplikasi sebagai aplikasi palsu dan kemudian menyebar dengan teknik *spearsphising.* Teknik penyebaran infeksi melalui komunikasi *email*, SMS, media sosial. Teknik ini menduplikasi seolah-olah berasal dari rekan kerja atau teman yang dikenal korban sebelumnya**.** Begitu korban mengunduh aplikasi palsu tersebut, *malware Dark Caracal* akan berjalan otomatis di *smartphone*, sementara pengguna tak menyadarinya. Per awal tahun ini, *malware Dark Caracal* sudah menginfeksi korban di 21 negara, mulai dari negara maju sampai negara berkembang.
Selain *malware Dark Caracal* terdapat juga ancaman yang menyerang perangkat salular. Aplikasi yang sering kali membawa program jahat tersebut selalu berevolusi baik secara teknologi, teknik ekspolitasi, target korban, hingga tujuan yang ingin dicapai. Berikut adalah tren kasus malware di perangkat selular selain malware Dark Caracal yang di kemukakan oleh perusahan perusahaan keamanan duania Kespersky, menyebutkan malware yang akan tren di tahun 2018.

1. Rooting malware

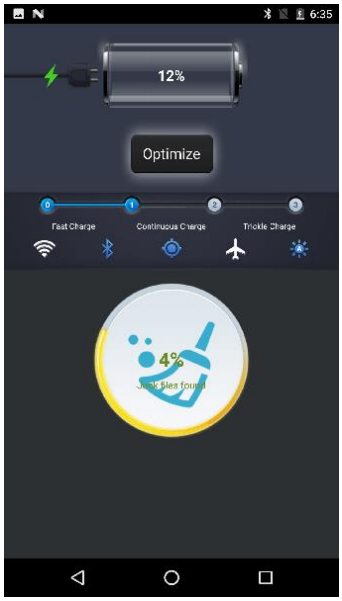
Rooting malware telah menjadi ancaman terbesar bagi pengguna *Android*. *Trojans* ini sulit untuk dideteksi, kemampuannya terus-menerus meningkat dan telah sangat populer di kalangan penjahat *cyber*. Tujuan utama mereka adalah untuk menunjukkan kepada para korban sebanyak mungkin iklan dan secara diam-diam memasang dan meluncurkan aplikasi yang diiklankan. Dalam beberapa kasus, tampilan agresif iklan *pop-up* dan penundaan dalam mengeksekusi perintah pengguna dapat membuat perangkat tidak dapat digunakan.



Gambar 2. Rooting Malware (Kaspersky)

2. WAP Trojan

WAP Billing merupakan suatu bentuk pembayaran seluler yang membebankan biaya langsung ke tagihan telepon seluler pengguna sehingga mereka tidak perlu mendaftarkan kartu atau menyiapkan nama pengguna dan kata sandi. Mekanisme ini mirip dengan SMS tarif premium, tetapi WAP Trojans yang mentarget WAP Billling tidak perlu mengirim SMS apa pun dalam kasus ini - mereka hanya perlu mengklik tombol pada halaman web dengan WAP-billing.



Gambar 3. WAP Trojan (Kaspersky)

3. Perkembangan dinamis dari Trojan Perbankan

Dunia mobile banking yang terus berkembang sepanjang tahun 2017, menawarkan cara-cara baru untuk mencuri uang. Kaspersky menemukan modifikasi dari aplikasi banking palsu *FakeToken* yang menyerang tidak hanya aplikasi keuangan tetapi juga aplikasi untuk memesan kendaraan, hotel, tiket, dll. *Trojan* tersebut bekerja dengan cara menumpuk antarmuka aplikasi dengan jendela *phishing* (teknik pencurian data dengan cara mengelabui pengguna untuk memasukkan data-data penting). Di sini, pengguna diminta untuk memasukkan rincian kartu bank mereka dan melakukan duplikasi akun bank.

Indonesia menempati peringat ketiga dalam hal serangan malware dimana 41,14 % pengguna mobile terkena serangan aplikasi jahat tersebut. Peringkat pertama diduduki Iran, dimana separuh lebih pengguna seluler di negara tersebut (57,25%) terkena serangan malware. Di bawahnya muncul negara Bangladesh dimana (42, 76%) pengguna seluler terkena serangan.

	Country*	%**
1	Iran	57.25
2	Bangladesh	42.76
3	Indonesia	41.14
4	Algeria	38.22
5	Nigeria	38.11
6	China	37.63
7	Côte d'Ivoire	37.12
8	India	36.42
9	Nepal	34.03
10	Kenya	33.20

Gambar 4. Peringkat negara dengan serangan malware tertinggi (securelist.com)

4. PENCEGAHAN DAN PENAGULANGAN SERANGAN SIBER

Aktivitas kejahatan siber dengan menyerang perangkat selular dengan program jahat atau melalui jaringan salular disebut dengan *cybercrime.* Banyak pola dancara yang bias dilakukan oleh para pelaku untuk melakukan serangan dan ada kiat-kiat dalam mencegah terjadinya *cybercrime*. Berikut cara untuk mencegah dan menghindari *cybercrime.*

1. Menggunakan Security Software yang Up to date
2. Melinsungi perangkat salular
3. Membuat password yang sulit
4. Membuat Salinan *(backup)*
5. Tidak sembarang Mngklik Link yang muncul di Sosial Media
6. Mengganti password secara berkala

Indonesia sendiri dalam menanggulangi tindak kejahatan di bidang teknologi sudah dicoba melalui beberapa cara, sebagai contoh pemerintah sudah membuat Undang- Undang ITE (Undang-Undang tentang Informasi dan Transaksi Elektronik), namun Undang-Undang ini akan tidak berguna apabila tidak di terapkan secara serius, dan apabila tidak disertai kesadaran masyarakat maupun aparat mengenai pentingnya kesadaran akan pencegahan di dunia maya. menurut penulis beberapa hal yang harus di lakukan untuk pencegahan peningkatan *cybercrime* di indonesia adalah sebagai berikut:

1. perlu adanya Undang-Undang yang kuat yang mengatur mengenai tindak kejahatan dibidang TI, serta komitmen pemerintah dan masyarakat dalam menjalankanya.
2. Pemerintah juga harus proaktif dalam melakukan diplomasi atau pun kerjasama dalam bidang hukum maupun TI dengan negara-negara lain, karena tidak menutup kemungkinan pelaku *cybercrime* berasal dari negara lain. dan dengan adanya kerja sama maka semakin kuat lah penerapan Undang-Undang yang berlaku.
3. Perlu ada nya evaluasi berkala dan tidak menutup kemungkinan akan ada nya perubahan Undang-Undang mengenai *Cybercrime*, hal ini dikarenakan Tingkat perkembangan Teknologi yang sangat pesat, sehingga sangat diharuskan agar Undang-Undang tetap bisa bertahan/ beradaptasi dengan perkembangan teknologi yang ada.
4. Meningkatkan penggunaan teknologi yang lebih aman, dan di sertai peningkatan sumber daya manusia dalam mengelolanya, sehingga memperkecil celah keamanan yang bisa di manfaatkan oleh para *cybercrime*

5. Menanamkan kesadaran akan bahayanya *cybercrime* dan bagaimana menanggulangi nya kepada masyarakat, sehingga mengurangi kesempatan para *cybercrime* dalam memanfaatkan kelengahan masyarakat dalam menggunakan teknologi

5. SIMPULAN

Dari pembahasan diatas dapat ditarik kesimpulan :

1. *Cybercrime* merupakan perbuatan yang merugikan, korban menganggap atau memberi stigma bahwa pelaku *Cybercrime* adalah penjahat.
2. Pengguna android sebaiknya mendownload aplikasi android dari situs terpercaya, dan sebelum memutskan menginstal aplikasi sebaiknya memeriksa terlebih dahulu dengan anti virus apakah aplikasi tersebut mengandung malware, serta terlebih dahulu memeriksa izin akses yang dijalankan oleh aplikasi.
3. Sistem perundang-undangan di Indonesia belum mengatur secara khusus mengenai kejahatan komputer melalui media internet. Beberapa peraturan yang ada baik yang terdapat di dalam KUHP maupun di luar KUHP untuk sementara dapat diterapkan terhadap beberapa kejahatan, tetapi ada juga kejahatan yang tidak dapat diantisipasi oleh undang-undang yang saat ini berlaku.

DAFTAR PUSTAKA

Amal Nur Ngazis “Virus Dark Caracal” *https://www.viva.co.id/digital/digilife/999921-waspada-virus-dark-caracal-penyusup-android-di-21-negara> (diakses 8 agustus 2018)*

A.P. Felt et al., “A Survey of Mobile Malware in theWild,”Proc. ACM Workshop Security and Privacy in Mobile Devices(SPMD 11), ACM, 2011, pp. 3-14.

Chris Mitchell, 2015 “ The cyber crime threat on mobile devices”, Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK

Gregory, Thomas HA, 2005 ”Ketenaran Cybercrime di Indonesia”, Makalah STIMIK Perbanas 2005 yang dipublikasikan diakses pada 8 agustus 2018 di www.google.com

K. Sharma,T. Dand, T. Oh, W. Stackpole, “Malware Analysis for Android operating”, 8th Annual Symposium on Information assurance , pp. 31-35, June 4-5, 2013

Hanna Mohamad, “ Background paper: mobile phone crime, 2011.