TINDAKAN PENCEGAHAN PROAKTIF BAGI PERLINDUNGAN APLIKASI ANDROIDDARI ANCAMAN 'MALWARE'

Muhammad Lokmanhakkim Salleh, Shahreza Shahril, Mohd Zamri Murah
Universiti Kebangsaan Malaysia
Bangi, Selangor, Malaysia
luqman505@gmail.com, ibnramadhan@gmail.com, mohdzamrimurah@gmail.com

ABSTRAK

Android pada masa kini telah digunakan dengan meluas oleh kebanyakan pengeluar peranti telefon pintar dan "tablet". Faktor utama yang menyumbang kepada fenomena ini adalah kerana ianya adalah perisian sumber terbuka dan boleh digunakan secara percuma oleh mana-mana pihak. Berbeza pula dengan pesaingnya yang terdekat iaitu iOS yang hanya boleh digunakan oleh peranti keluaran Apple. Walau bagaimana pun, disebalik populariti dan fungsi-fungsi menarik yang terdapat pada Android, terdapat statistik yang menunjukkan serangan malware kepada sistem pengoperasian mobil ini telah menunjukkan peningkatan yang ketara pada setiap tahun. Perkara ini telah meletakkan Android bukan sahaja sebagai sistem pengoperasian yang paling meluas dan popular, tetapi juga ia juga dilabelkan sebagai sistem pengoperasian yang paling berisiko dengan serangan malware. Google sebagai pembangun utama Android telah cuba mempertingkatkan fungsi-fungsi keselamatan dengan mengeluarkan versi-versi baru yang dikemaskini. Walaubagaimana pun setakat ini, statistik terus menunjukan peningkatan kes serangan malware kepada Android. Sebagai alternatif kajian ini akan mencadangkan beberapa langkah pencegahan proaktif yang boleh dilaksanakan untuk melindungi pengguna sistem Android daripada mengalami impak yang teruk daripada serangan malware.

Keywords: *Android, mobile malware, mobile security.*

---

1. Pengenalan

Android adalah sistem pengoperasian mobile yang berada pada ranking pertama dunia berdasarkan laporan bertajuk "*Worldwide Smartphone Sales to End Users by Operating System in 2013*" oleh Gatner. Laporan tersebut menyatakan jumlah jualan telefon pintar berasaskan Android adalah sebanyak 758,719.90 unit berbanding jumah yang dicatatkan bagi tahun 2012 iaitu sebanyak 451,621 unit. Jumlah ini telah meninggalkan jauh pesaing terdekat Android iaitu iOS yang hanya mencatakan jualan sebanyak 150,785.9 unit bagi tahun 2013. Faktor utama yang menjadikan Android mendapat tempat dikalangan pengeluar dan penguna peranti Android adalah kerana ianya merupakan sistem sumber terbuka yang dibangunkan oleh Google dan bebas digunakan secara percuma oleh mana-mana pengeluar telefon pintar dan *tablet* berbanding iOS yang penggunaanya hanya terhad kepada peranti yang dikeluarkan oleh syarikat Apple. Populariti dan dominasi pasaran oleh Android ini telah menjadikan ianya tumpuan serangan *malware*sama seperti yang berlaku kepada sistem pengoperasian Windows yang mendominasi pasaran komputer peribadi dan komputer riba. Kebanyakkan *malware* yang dikesan menggunakan aplikasi-aplikasi percuma yang boleh dimuat turun daripada stor aplikasi rasmi Android iaitu Google Play atau melalui laman web yang dibina oleh pihak ketiga sebagai medium utama penyebaran *malware*. Serangan *malware* telah mendatangkan kesan yang buruk kepada peranti dan pengguna Android. Langkah pencegahan perlu diambil

untuk mengawal kesan sebaran daripada menjadi lebih buruk kerana serangan *malware* bagi Android dijangkaakansentiasa meningkat pada setiap tahun.

2. Kajian Literatur

Peningkatan penggunaan dan pendedahan awal teknologi telefon pintar berasaskan sumber terbukaterhadap pengguna menyebabkan meningkatnya risiko keselamatan sistem aplikasi yang digunapakai. Android dilihat hanya menyediakan set fungsi kebenaran (*permission*) asas untuk melindungi aplikasi telefon pintar. Jika dilihat dari aspek praktikaliti, teknik tersebut diimplementasi bagi menjadikan mekanisme keselamatan Android lebih fleksibel. Namun begitu, pada masa yang samaianya menyebabkan mekanisme keselamatansemasa yang diaplikasikan menjadi terlalu terhad. Pengguna hanya mempunyai dua pilihan bagi pemasangan aplikasi samaada membenarkan semua kebenaran (*permission*) yang diminta atau tidak membenarkan permintaan tersebut dan menghentikan pemasangan aplikasi. (S. Powar, Dr. B. B. Meshram,2013)

3. Kaedah Kajian, Analisa, Dapatan dan Cadangan Penyelesaian

3.1 Kaedah Penyelidikan

Kajian ini adalah berdasarkan analisa yang dibuat melalui dua laporan iaitu "*Cisco Annual Security Report 2014*" dan "*Sophos Mobile Security Threat Report 2014*". Analisa dibuat adalah bertujuan untuk melihat corak semasa serangan *malware* yang menyerang sistem Android. Data yang diperolehi daripada analisa kepada kedua-dua laporan berkenaan akan dijadikan asas kepada cadangan langkah pencegahan proaktif bagi melindungi aplikasi Android daripada serangan *malware*.

3.2 Analisa Laporan

3.2.1 Jumlah Serangan *Malware*

Hasil analisa kedua-kedua laporan mendapati 99 peratus *malware*telah menyerang peranti Android berbanding sistem pengoperasian lainsekaligus mencatatkan jumlah serangan *malware* tertinggi bagi tahun 2013. Laporan merekodkan sebanyak 650,000 *malware* dikesan sepanjang 2013 dengan anggaran 1000 *malware* baru dikesan pada setiap hari.

3.2.2 Sasaran Serangan

Sasaran utama bagi *malware* yang dikesan sepanjang 2013 adalah aplikasi-aplikasi Android yang terdapat di dalam aplikasi Google Play dan juga yang boleh dimuat turun tanpa sekatan khusus daripada laman web pihak ketiga. Kebanyakan aplikasi tersebut ditawarkan secara percuma bagi menarik minat pengguna untuk memuat turun aplikasi ke dalam peranti mereka.

3.2.3 Tujuan serangan

Terdapat beberapa tujuan serangan *malware* yang dikenalpasti, antaranya adalah seperti berikut:

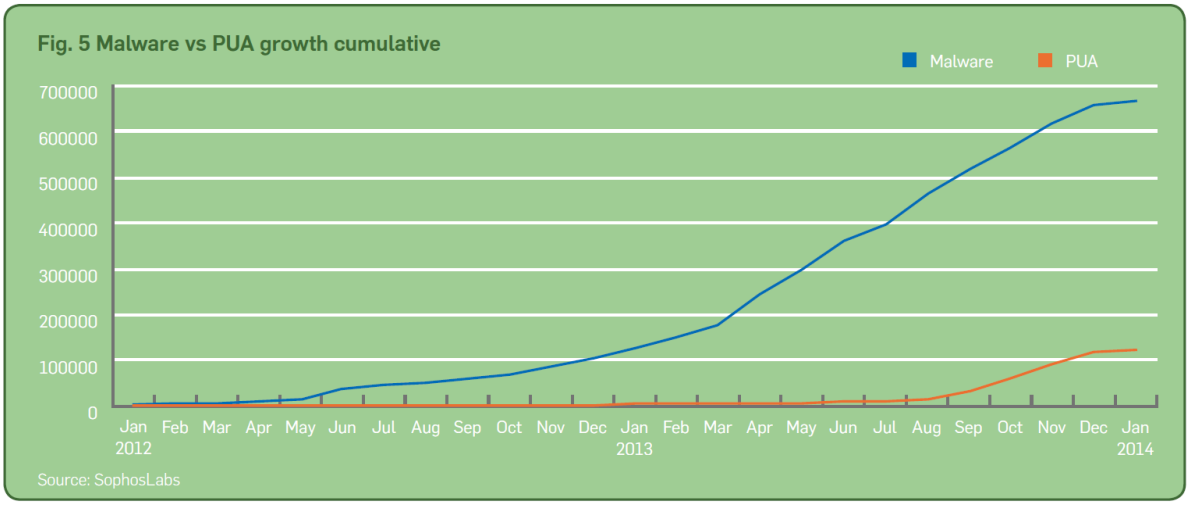
i) Mencuri data peribadi seperti maklumat akaun bank dan laman sosial;
ii) Mengaut keuntungan secara tersembunyi melalui khidmat pesanan ringkas (SMS) dan membuat panggilan telefon secara tidak sah kepada nombor yang mengenakan kadar premium;
iii) Menyebabkan kerosakan kepada peranti pengguna.

3.2.4 Bentuk *Malware* yang Lebih Kompleks

Terdapat jenis *malware* yang dikesan 25 tahun lepas telah kembali digunakan bagi menyerang peranti berasaskan Android. *Malware* yang dikenali dengan *ransomware* ini menggunakan kaedah memaksa pengguna yang dijangkiti bagi membayar sejumlah wang bagi membolehkan peranti Android yang telah dikuasai digunakan kembali. Bentuk *malware* ini dilihat lebih kompleks apabila ianya mampu menyahaktifkan fungsi-fungsi utama peranti termasuk pilihan "*back*" dan "*home*" selagi mana pengguna tidak menjelaskan bayaran yang diminta.

3.2.5 Pontetially Unwanted Program (PUA)

PUA bukanlah daripada kategori *malware*, walaubagaimanapun, seperti carta diRajah 1 di bawah menunjukkan wujudnya peningkatan kes yang melibatkan PUA. PUA merupakan aplikasi Android yang mewujudkan pautan tidak selamat serta mengandungi iklan-iklan dan maklumat yang tidak diperlukan pengguna. PUA berpontensi bagi menyebarkan iklan berkaitan pronografi demi mengaut keuntungan.Selain itu,ia juga mampumenjejak peranti pengguna beserta lokasi, malah mampu memanipulasi maklumat senarai nombor telefon di dalam peranti penggunabagi digunakan untuk tujuan yang salah.



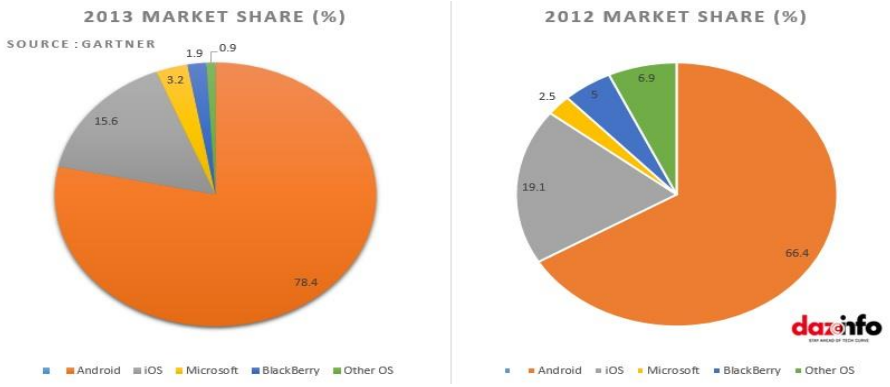
Rajah 1: Perbandingan Perkembangan *Malware* dan PUA Bermula dari Januari 2012 hingga Januari 2014(Sumber: Sophos Mobile Threat Report 2014)

3.3 Dapatan Kajian

Berdasarkan analisa terhadap dua laporan tersebut. Terdapat beberapa sebab utama yang telah dikenal pasti yang menyebabkan sistem Android menjadi sasaran serangan *malware* iaitu seperti berikut:

i) Dominasi Pasaran

Seperti carta pai di Rajah 2 menunjukan Android telah menguasai pasaran bagi penjualan peranti telefon pintar dan tablet yang menyebabkan penjenayah siber cenderung bagi menjadikannya sebagai pusat serangan *malware*.



Rajah 2: Perbandingan Menunjukkan Penguasaan Pasaran Perisian Android Berbanding Sistem Pengoperasian Lain Bagi Tahun 2012 dan 2013 (Sumber: Gatner)

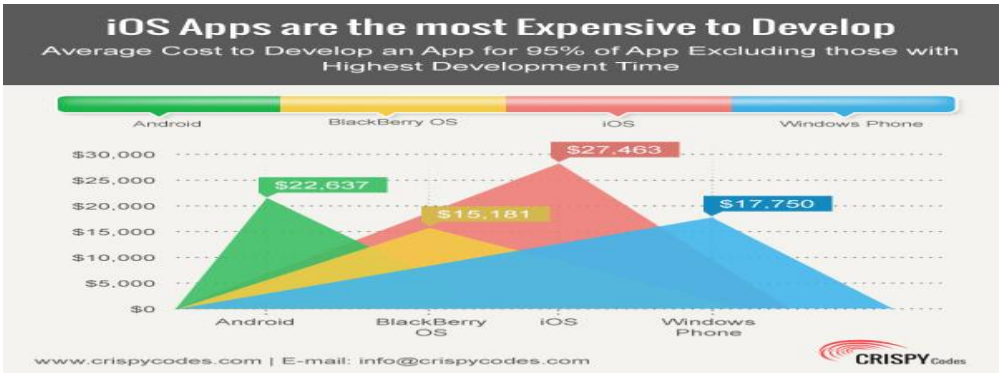
ii) Sistem Sumber Terbuka.
Google telah membangunkan dan meletakkan Android sebagai sistem yang berasakan sumber terbuka. Ianya bebas digunakan oleh pelbagai pihak secara percuma. Oleh itu, pengeluar peranti telefon pintar dan tabletdilihat cenderung untuk menggunakan sistem ini sebagai platform utama produk mereka. Polisi ini jelas berbeza dengan iOS yang mempunyai polisi tertutup bagi penggunaan sistem pengoperasiannya yang hanya terhad kepada peranti yang dikeluarkan oleh syarikat Apple sahaja. Pendekatan yang diperkenalkan syarikat Google ini membolehkan kod sumber (*source code*) dimanipulasi bagi penyebaran *malware*.

iii) Kewujudan Aplikasi Daripada Sumber Ketiga
Walaupun Android mempunyai perkhidmatan gedung aplikasi rasminya tersendiri iaitu Google Play, namun pihak Google tidak mempunyai peruntukan khas untuk menyekat kewujudan gedung aplikasi lain yang dibangunkan oleh pihak ketiga. Aplikasi Android juga boleh dimuat turun daripada laman web yang dibangunkan oleh pihak ketiga. Perkara ini menyebabkan penyebaran *malware*menjadi tidak terkawal. Pembangun aplikasi menggunakan tarikan-tarikan tertentu seperti aplikasi permainan yang menarik atau aplikasi yang menawarkan fungsi-fungsi untuk meningkatkan keterujaan pengguna tanpa memikirkan risiko*malware*berbahaya yang terembunyi disebalik aplikasi tersebut.

iv) Mobiliti
Penyebaran *malware* adalah lebih mudah diperluaskan di dalam sistem Android memandangkan ianya digunakan oleh telefon pintar dan tablet yang bersifat mobil dan sentiasa berhubung dengan rangkaian. Secara umumnya pengguna akan memperuntukkan masa yang lebih bagi mengunakan telefon pintar dan tablet berbanding PC atau *notebook* yang kegunaanya terhad kepada masa dan tempat tertentu. Peranti telefon dan tablet yang bersifat lebih kecil dan mudah dibawa menyumbang kepada faktor tersebut. Apabila penggunaannya adalah lebih kerap maka peluang dan ruang bagi penyebaran *malware* adalah lebih tinggi.

v) Kos yang rendah
Google telah meletakkan Android sebagai sistem terbuka dan percuma. Pelbagai pengeluar peranti telefon pintar dan tablet menggunakan sistem Android sebagai

sistem pengoperasian peranti mereka. Tambahan pula kebanyakan aplikasi Android yang ditawarkan di Google Play adalah percuma. Peluang ini digunakan oleh penjenayah siber bagi menyebarkan *malware*dengan cara membangunkan pelbagai bentuk aplikasi yang kelihatan tidak berisiko tetapi hakikatnya ianya mempunyai agenda tersembunyi di mana pembangun aplikasi tersebut mungkin telah menyembunyikan *trojan* atau *botnet* bagi mendapatkan maklumat-maklumat penting pengguna tanpa diketahui. Rajah 3 menunjukan perbandingan kos pembangunan aplikasi mobil.



Rajah 3: Perbandingan Kos Bagi Pembangunan Aplikasi Mobil Beradasarkan Jenis Sistem Pengoperasian. (Sumber: http://www.crispycodes.com)

vi) Ketandusan maklumat

Pada masa kini maklumat berkenaan *malware* yang menyerang Android sukar di dapati secara kolektif dan interaktif. Situasi ini menyebabkan maklumat awal sukar diperolehi oleh pengguna bagi membolehkan mereka mengelak daripada terjerat dengan perangkap *malware* yang berisiko mendatangkan masalah kepada peranti Android mereka.

3.4 Cadangan Penyelesaian Masalah

Berdasarkan maklumat dan hasil analisa yang telah dilakukan, tindakan pencegahan yang proaktif perlu dilaksanakan bagi mengawal penyebaran *malware* secara berleluasa. Tindakan pencegahan dilihat lebih relevan berbanding tindakan penghapusan yang dilihat agak mustahil kerana penyebaran dan pembangunan *malware* adalah bersifat pelbagai dan tidak mempunyai mekanisme yang tetap. Terdapat tiga pihak utama yang perlu memainkan peranan dalam memastikan langkah pencegahan ini dapat dilaksanakan dengan berkesan iaitu:

i) pemilik atau pembangun Android iaitu Syarikat Google
ii) pengeluar peranti telefon pintar dan tablet berasaskan Android
iii) pengguna sistem Android

Pencegahan bermaksud melaksanakan mekanisme pengawalan bertujuan untuk menghadkan pengeluasaan *malware*. Proaktif bermaksud bertindak mendahului kejadian di mana tindakan yang diambil adalah bersifat jangkaan awal sebelum keadaan sebenar berlaku. Ini dapat dilakukan dengan mengkaji gaya, corak dan kesan *malware*sedia ada dan membuat jangkaan mengenai serangan baru yang mungkin dilakukan oleh penjenayah siber.

Perlaksanaan tindakan ini bergantung kepada kesedaran setiap pihak yang terlibat bagi memastikan peranan yang dimainkan dapat menghasilkan kaedah pencegahan yang lebih positif. Tindakan ini dijangka mampu mengurangkan risiko penyebaran dan jangkitan *malware* kepada sistem Android.

Tindakan yang dicadangkan adalah seperti berikut:

i) Pemilik atau pembangun sistem pengoperasian Android (Google)
Sebagai pemilik atau pembangun utama Android, pihak Google dicadangkan mengambil langkah-langkah berikut sebagai langkah proaktif bagi mengawal penyebaran *malware* ke peranti berasaskan Android:

a) Menghadkan muatturun dan pembelian aplikasi Android hanya melalui Google Play sahaja.
Mencipta atau meminda polisi baharu iaitu dengan menghadkan proses muatturun aplikasi bagi Android hanya daripada Google Play sahaja. Ini bertujuan bagi mengurangkan risiko penyebaran *malware* daripada sumber pihak ketiga yang mungkin hanya aplikasi palsu yang mengelirukan pengguna. Dengan adanya stor aplikasi tunggal ini kawalan dan pemantauan kepada aplikasi adalah lebih mudah dilakukan.

b) Mewujudkan *trusted badge* bagi aplikasi yang sah
"*Trusted badge*"ataupun tanda pengesahan bagi aplikasi di Google Play yang bermaksud aplikasi tersebut telah disemak dan disahkan bebas oleh pihak Google daripada unsur-unsur *malware* yang boleh mendatangkan risiko kepada pengguna Android. Setiap aplikasi yang melepasi piawaian yang ditetapkan akan ditandakan dengan satu tanda pengesahan atau "*trusted badge*" yang akan menjadi panduan kepada pengguna sebelum memuat turun aplikasi tersebut. Rajah 4 menunjukkan contoh "*trusted badge*" yang boleh diletakkan pada aplikasi yang telah disemak dan disahkan selamat untuk digunakan.

Rajah 4: Contoh *Trusted Badge*

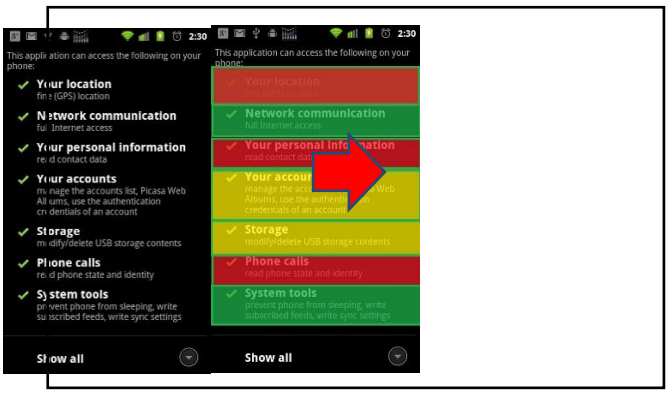
c) Menutup capaian kepada fungsi call dan SMS oleh pihak ketiga
Fungsi panggilan (*call*) dan sistem pesanan ringkas (SMS) adalah antara fungsi yang mampu dimanipulasi oleh *malware* bagi mendapatkan keuntungan secara tidak sah dengan membuat sambungan kepada talian *premium rate* yang mengenakan caj yang tidak munasabah. Oleh itu adalah amat wajar sekiranya pihak Google menyulitkan capaian kepada dua fungsi ini daripada dicapai oleh pihak yang tidak sepatutnya.

d) Mewujudkan forum komuniti keselamatan Android terbuka atas talian

Memandangkan kejadian serangan *malware* yang semakin kerap,adalah dirasakan perlu untuk diwujudkan satu forum komuniti keselamatan Android terbuka secara atas talian sebagai salah satu khidmat komuniti yang boleh diaplikasikan oleh Googlekepada pengguna Android. Pihak Google boleh menyelaras kewujudan forum ini dan menyelaraskan perbincangan di kalangan pakar dan pengguna Android bagi mendapatkan maklumat berhubung dengan *malware* dan langkah keselamatan berkaitan. Forum ini akan menjadi sumber rujukan kepada pengguna Android bagi membantu mereka berkongsi masalah dan mendapatkan penyelesaian bagi kesulitanyang dihadapi melibatkan *malware* dan isu – isu keselamatan. Meletakkan pakar security Android daripada pihak Google atau pihak yang berautoriti sebagai pengurus forum tersebut juga adalah satu inisiatif yang perlu dipertimbangkan.

e) Transformasi terhadap pengkategorian risiko bagi kebenaran capaian oleh aplikasi

Setiap bentuk kebenaran (*permission*) yang diperlukan oleh aplikasi yang dipasang oleh pengguna perlu ditandakan mengikut kategori warna bagi mewakli risikonya. Sebagai contoh warna hijau bagi kebenaran kategori risiko rendah, kuning bagi risiko sederhana dan merah bagi risiko tinggi. Rajah 5 menunjukan contoh transformasi kepada kebenaran (*permission*)bagi pemasangan aplikasi Android:



Rajah 5: Transformasi Bagi Kebenaran Instalasi Aplikasi

ii) Pengeluar peranti telefon pintar dan tablet berasaskan Android melaksanakan langkah pencegahan awal

Selain pembangun Android iaitu Google, pihak yang mengeluarkan peranti telefon pintar dan tablet perlu memainkan peranan mereka dalam memastikan penggunanya dapat mengawal kebanjiran *malware*daripada memanipulasi peranti yang dimiliki. Antara tindakan proaktif yang dicadangkan kepada pengeluar ialah:

a) menyertakan pakej aplikasi *malware scanning*khusus bagi peranti yang dibangunkan.Melalui kaedah ini, imbasan terhadap *malware* dapat dilakukan terutamanya bagi *entrypoint* yang paling berpotensi dijadikan pintu masuk bagi *malware* tersebut iaitu meliputisambungan wifi serta sambungan data 3G Internet yang dilanggan melalui pembekal perkhidmatan telekomunikasi.

Pakej imbasan *malware* tersebut perlulah disertakan dengan fitur tambahan seperti imbasan berjadual bagi storan dalaman dan juga storan luaran peranti.

iii) Pengguna Android perlu meningkatkan tahap kesedaran terhadap isu – isu keselamatan siber

Pihak pengguna juga mempunyai peranan yang perlu dimainkan dalam memastikan penyebaran *malware* di dalam peranti yang digunakan dapat disekat dengan berkesan. Antara langkah proaktif yang dicadangkan adalah:

a) Menyelidiki status aplikasi yang ingin dimuatturun

Pengguna boleh menyemak di internet atau forum khusus bagi mendapatkan pandangan pelbagai pihak yang telah memuat turun aplikasi yang dimahukan. Melalui kaedah ini pengguna dapat mengetahui status tahap keselamatan aplikasi tersebut samaada selamat atau tidak untuk digunakan.

b) Menjalankan *malware* scanning dalam sela masa tertentu

Pengguna perlu memastikan aplikasi*malware scanning* yang dimuat turun adalah dibangunkan oleh penyedia perkhidmatan keselamatan yang sah seperti Avira, McAfee dan sebagainya. Pada masa kini kebanyakan syarikat penyedia aplikasi keselamatan telah membangunkan versi instalasi Android yang kebanyakannya ditawarkan secara percuma. Selain itu, perlu dipastikan signature pada perisian yang dipasang telah dikemaskini. Disamping itu, pengguna juga perlu menjalankan imbasan berjadual seperti secara mingguan terhadap peranti tersebut.

c) Meningkatkan pengetahuan berkenaan risiko *malware*

Menjalankan sedikit kajian melalui semakan di laman web berkenaan *malware*yang berisiko menjangkiti Android mampu membantu meningkatkan pengetahuan pengguna. Apabila pengetahuan telah meningkat maka pengguna akan lebih berhati-hati dalam melakukan sesuatu tindakan terhadap peranti yang digunakan.

4.0 Kesimpulan

Langkah-langkah pencegahan proaktif yang dicadangkan di dalam kajian ini sekiranya dijalankan dengan bersepadu oleh ketiga-ketiga pihak yang telah dinyatakan dijangka mampu membantu di dalam mengurangkan kesan serangan *malware* kepada penguna peranti berasaskan Android. Walau bagaimana pun, pemerhatian dan pemantauan yang berterusan perlu terus dijalankan dalam memastikan sistem berasaskan Android adalah selamat digunakan memandangkan ianya semakin mendapat tempat dalam menjalankan urusan seharian samaada melibatkan urusan pejabat atau peribadi. Tambahan pula peningkatan keupayaan telefon pintar dan tablet berasaskan Android dilihat bakal mengantikan fungsi komputer peribadi dan komputer riba bagi menjalankan pelbagai bentuk urusan. Oleh itu keselamatan daripada sebarang bentuk ancaman seperti serangan *malware*tindak boleh dipandang ringan dan memerlukan perhatian yang berterusan daripada pihak-pihak yang terlibat.

Penghargaan
Beribu penghargaan kepada seluruh tenaga pengajar yang terlibat secara langsung dan tidak langsung daripada Cyber Security Malaysia (CSM) terutama buat En.MohdFadzlan bin Mohamed Kamal, En. Abdul Fuad bin Abdul Rahman, En. Mohammad Noorhisyam bin Muda dan En. Amiroul Farhan bin di atas segala bantuan dan tunjuk ajar yang diberikan di dalam memastikan kajian ini dilaksanakan dengan sebaiknya. Ribuan terima kasih juga di atas panduan dan pemerhatian yang diberikan oleh semua pensyarah di Unit Keselamatan Siber, Fakulti Teknologi dan Sains Maklumat (FTSM), Universiti Kebangsaan Malaysia (UKM).

Rujukan

Cisco (2013), "*Cisco 2014 Annual Security Report*",dicapai pada 15 Mei 2014, daripada https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

Gatner (2013), *"Worldwide Smartphone Sales to End Users by Operating System in 2013"*, dicapai pada 15 Mei 2014, daripadahttp://www.gartner.com/newsroom/id/2665715.

Rahul Vyas (2014),"*Application Development at iOS is Costly Compare to Android, Blackberry, Windows and Others",* dicapai pada 1 Julai 2014, daripada http://www.crispycodes.com/blog/mobile-app-development/application-development-ios-costly-compare-android-blackberry-windows-others.php.

Sophos (2014), "Sophos Mobile Security Threat Report 2014",dicapai pada 15 Mei 2014, daripadahttps://www.sophos.com/en-us/.../sophos-security-threat-report-2014.pdf.

Tiwari Mohini, Srivastava Ashish Kumar and Gupta Nitesh (2013), *"Review on Android and Smartphone Security"*, dicapai daripada http://www.isca.in/COM_IT_SCI/Archive/v1/i6/3.ISCA-RJCITS-2013-030.pdf.