REPOSITOR, Vol. 2, No. 8, Agustus 2020, Pp. 1163-1174
ISSN : 2714-7975
E-ISSN : 2716-1382

Analisis Malware Berdasarkan Tujuan Pembuatan Dengan Menggunakan Metode Hybrid Pada Android

Septian Dwi Kurnia*[1], Denar Regata Akbi*[2], Diah Risqiwati*[3]
[1,2,3]Teknik Informatika/Universitas Muhammadiyah Malang
septian.dk@webmail.umm.ac.id[*1], dregata.dosen@gmail.com[*2], diah.rizqiwati@gmail.com[*3]

Abstrak

Malware android adalah salah satu permasalahan yang kini marak diperbincangkan oleh pengguna, alasannya adalah karena sebagian besar waktu yang dimiliki masyarakat digunakan untuk berinteraksi dengan dunia maya. Perkembangan malware dari hari ke hari mulai terlihat, malware yang awalnya terdapat pada sistem komputer kini mulai masuk ke ranah Smartphone. Tidak lagi diperuntukan untuk merusak Malware kini hadir dengan berbagai macam jenis dan kegunaan. Penelitian demi penilitian muncul membahas bagaimana mengatasi pergerakan malware yang kian pesat mulai dari meningkatkan kualitas deteksi dengan menggabungkan algoritma deteksi dinamis dan statis hingga menggunakan bantuan Machine learning. Dari sekian banyak penelitian tersebut muncul pengkategorian pada Malware dengan tujuan memudahkan penelitian. Pengkategorian tersebut selalu berubah – ubah dari tahun ke tahun alasannya karena banyaknya Malware yang muncul tiap harinya. Pada penelitian kali ini penulis berkesempatan untuk membahas perkembangan dari malware berdasarkan tujuan pembuatan nya atau kategori dari malware itu sendiri. Penilitian ini akan melibatkan analisis hybrid dengan menggunakan parameter dari perilaku Malware sehingga dapat diketahui sejauh mana malware telah berkembang.

Kata Kunci: *Virus Android, Malware, Deteksi Malware, Kategori Malware, Perilaku Malware*

Abstract

Android malware is one of the problems that is now widely discussed by users, the reason being that most of the time people have is used to interact with cyberspace. The development of malware from day to day began to be seen, malware that was originally found on a computer system is now beginning to enter the realm of smartphones. No longer intended to damage Malware now comes with various types and uses. Research for the sake of research appears to discuss how to deal with the increasingly rapid movement of malware ranging from improving the quality of detection by combining dynamic and static detection algorithms to using Machine learning. Of the many studies that emerge categorizing Malware with the aim of facilitating research. Categorization is always changing - change from year to year the reason because of the many Malware that appear every day. In this study the author had the opportunity to discuss the development of malware based on the purpose of its creation or the category of malware itself. This research will involve hybrid analysis using parameters of Malware behavior so that it can be seen how far the malware has developed.

Keywords: *Android Viruses*, *Malware, Malware Detection, Malware Category, Malware Behaviour*

1. Pendahuluan

Smartphone adalah sebuah perangkat elektronik yang menjadi hal penting bagi kebanyakan masyarakat, hampir segala aktivitas yang berhubungan dengan dunia maya sudah dapat dilakukan melalui smartphone. Smartphone memegang peranan yang begitu banyak di era digital ini, diantaranya menjadi wadah untuk menyimpan berbagai data pribadi seperti video, gambar, dokumen penting dan data lainnya[1]. Industri smartphone dengan sistem operasi berbasis android berada diperingkat atas sebagai sistem operasi yang paling banyak digunakan dalam pengembangan di pasaran dengan tingkat penyebaran di pasaran mencapai 70 – 80% sejak peluncurannya pada tahun 2008 [2] .Alasan sistem operasi android dapat mencapai tingkat teratas dipasaran adalah karena penggunaan sistem arsitektur terbuka terbuka yang membebaskan para pengembang untuk mempelajari dan membangun software sesuai yang

diinginkan, oleh karena itu mudah bagi sistem Android menarik perhatian bagi seluruh kalangan industri. Menggunakan sistem arsitektur terbuka tentu memiliki banyak keunggulan didalamnya, namun dilain sis hal tersebut juga memiliki sebuah resiko didalamnya salah satu resikonya adalah serangan dari sebuah *Malware (Malicious Software)*. Karena dengan membuat sistem arsitektur terbuka secara tidak langsung sistem *Android* juga membebaskan pihak pengembang *Malware* untuk turut serta mengembangkan *Malware* pada sistem operasi tersebut.

Malware atau *Malicious Software* lebih dikenal oleh masyarakat sebagai virus, sebuah bagian kecil dari sebuah program yang masuk ke dalam perangkat tanpa diketahui oleh pengguna dan program tersebut berlawanan dengan sistem perangkat dari ponsel tersebut [3]. Dijelaskan oleh Monika, P. Zavarsky, and D. Lindskog adapun beberapa poin penting dari malware yang berbahaya dari *Malware* diantaranya privilege escalation, remote control dan information colletion [4]. Ketiga hal tadi merupakan beberapa contoh dari tindakan yang dapat dilakukan oleh suatu *Malware* apabila perangkat telah terinfeksi oleh sebuah malware.

Berdasarkan pengetahuan umum yang diketahui oleh masyarakat sebuah *Malware* adalah program yang akan merusak data mereka apabila perangkat yang dimiliki telah terinfeksi, tapi pada kenyataannya jika dilihat dari perkembangannya *Malware* tidak lagi digunakan untuk merusak sebuah data. Karena telah dijumpai banyaknya kasus pada perangkat android yang menyatakan sebuah *Malware* digunakan untuk kasus – kasus lain seperti yang dijelaskan pada paragraph sebelumnya. Pengembangan ke arah tersebut dinilai lebih menguntungkan dari sudut pandang pengembang *Malware,* sehingga mulailah bermunculan berbagai jenis *Malware* dengan tujuan yang berbeda. Kemunculan berbagai jenis *Malware* tersebut membawa dampak pada masyarakat yang akhirnya membuat banyak penelitian bermunculan mulai dari analisis perilaku hingga menemukan cara paling efektif untuk mendeteksi keberadaan malware. Adapun beberapa penelitian dibawah ini yang memiliki hubungan dengan banyaknya kemunculan malware.

Beberapa penelitian yang berkaitan dengan *Malware* diantaranya penelitian oleh Ignacio tentang "*Machine-Learning based analysis and classification of Android Malware Signatures*"[5] menjelaskan penggunaan *signature* yang didapat pada malware dan digabungkan dengan algoritma *Machine Learning* untuk menganalisis penyebab kesalahan pendeteksian sebuah antivirus terhadap beberapa aplikasi yang tidak tergolong malware. Penelitian selanjut oleh Yaocheng tentang "*SaaS: A Situational Awareness and Analysis System for Massive Android Malware Detection*"[6] penelitian ini membahas tentang pengembangan pendeteksian malware pada sistem *Cloud* dengan menggabungkan analisis statis dengan 3 metode lain yaitu metode pemrosesan bahasa (n –gram), fuzzy, dan *machine learning.* Pada prosesnya mereka melakukan analisis statis dan metode pemrosesan bahasa guna mendapatkan data yang selanjutnya dengan algoritma *machine learning* dibuatkan sebuah data latih untuk membuat model pendeteksi, model pendeteksi ini akan diperkuat dengan menggunakan teknik fuzzy untuk mendeteksi apakah aplikasi yang sedang diinspeksi tengah dikemas atau tidak.

Sebagian besar penelitian yang ada hanya membahas bagaimana cara mengatasi malware yang telah bermunculan seperti kedua pembahasan jurnal diatas. Sedangkan pembahasan tentang perkembangan dan seperti apa malware dimasa sekarang dan untuk jangka waktu kedepan nya masih dikatakan sedikit dan salah satunya Adalah penelitian oleh Chakkaravarthy, Sangeetha, dan Vaidehi dimana didalam penelitiannya disajikan proses lengkap yang mudah dipahami untuk melihat kluster ancaman dan celah untuk menemukan dampak yang berbahaya pada masyarakat dan meneliti dari sudut pandang pengganggu, dibandingkan berbagai teknik pencegah yang digunakan secara transparan oleh pembuat *Malware* untuk menghambat upaya pendeteksian. untuk mengurangi atau menghindari dampak berbahaya di masa depan [7].

Pada tahun 2016 di jurnal yang ditulis oleh Sapna dan Kiran dengan judul "*Sytem call Analysis of Android Malware Families*" membahas tentang perubahan perilaku *Malware* pada tahun 2011 dan 2012 dengan menggunakan teknik analisis dinamis dengan menggunakan sistem pemanggilan sebagai parameter penilaian perubahan *Malware* tersebut dimana ditunjukkan bahwa dari banyaknya *Malware* yang diteliti dari tahun 2011 hingga 2012 terdapat sebuah perubahan perilaku pada *Malware* tersebut [8]. Namun pada penelitian tersebut ditemukan bahwa hanya terdapat 2 kategori dari sekian data yang dianalisis. Dimana penelitian ini yang menjadi alasan awal peneliti ingin mengetahui perkembangan malware pada saat ini.

Pada tahun yang sama Dina , El-Gokhy, dan Sallam pada penelitian tentang penggunaan framework Deep Belief Network untuk mendeteksi *Malware* pada sistem android dikatakan bahwa bahwa pada tahun 2016 google mengatakan terdapat setidaknya 12 kategori yang

berbeda yang ada pada malware [9] melihat dari hal tersebut penulis ingin tahu lebih dalam tentang perkembangan malware yang terjadi pada masa saat ini dan dan apakah terdapat kemungkinan munculnya malware kategori baru di masa sekarang, karena kemungkinan munculnya sebuah *Malware* dengan kategori baru sangat mungkin terjadi karena perkembangan teknologi yang semakin besar adanya.

Untuk mengetahui perkembangan malware dalam hal kategori pada kesempatan kali ini penulis berkeinginan melakukan penelitian tentang melihat perkembangan tersebut yang melibatkan proses dengan membandingkan data berdasarkan pada kategori data 2016 dan data dimasa sekarang yang membedakan penelitian ini dengan dengan penelitian serupa adalah pada penelitian ini membahas perkembangan dari malware berdasarkan kategori dengan menggunakan analisis hybrid dimana penelitian sebelumnya hanya menggunakan proses analisis dinamis. Proses penelitian dilakukan dengan mendapatkan data berupa pola perilaku yang kemudian akan dibandingkan dan dilihat perbedaan nya berdasarkan kategori dan tahun. Parameter yang digunakan dalam uji analisis ini adalah pola perilaku dari malware yang didapat dari proses penelitian secara dinamis dan statis. Untuk memudahkan penelitian penulis menggunakan Emulator android dan beberapa tools, seperti Strace untuk membantu melakukan proses analisis dinamis dan 2 Library java yaitu RAPID.jar serta AXMLprinter.jar untuk membantu dalam proses analisis statis.

Naskah wajib dikirim melalui website http://kinetik.umm.ac.id dengan alur registrasi yang sudah ditentukan. Seluruh proses pendaftaran dan pengiriman naskah tidak dipungut biaya. Panjang naskah minimal 8 halaman dan maksimal 12 halaman. A4 (210 x 297 mm), dengan format naskah sesuai template yang disediakan. Naskah ditulis menggunakan Microsoft Word (.doc) dengan batas atas, kanan, bawah, kiri 30 mm

2. Metode Penelitian

Berdasarkan dari penelitian-penelitian terdahulu terkait analisis *Malware*, kebanyakan penelitian hanya membahas perbandingan algoritma dan cara lebih efisien untuk mendeteksi sebuah *Malware* namun dari sekian banyak penelitian masih tergolong sedikit penelitian yang membahas bagaimana atau seperti apa perubahan *Malware* yang ada. Seperti penelitian yang diangkat oleh penulis saat ini adalah tentang bagaimana perubahan perilaku *Malware* pada ketegori dari tahun 2016 sampai tahun 2019 apa saja yang telah berubah dan apakah terdapat kemunculan kategori baru dari sebuah *Malware*. Target penulis disini untuk mengetahui perkembangan atau perubahan tersebut berdasarkan kategori.

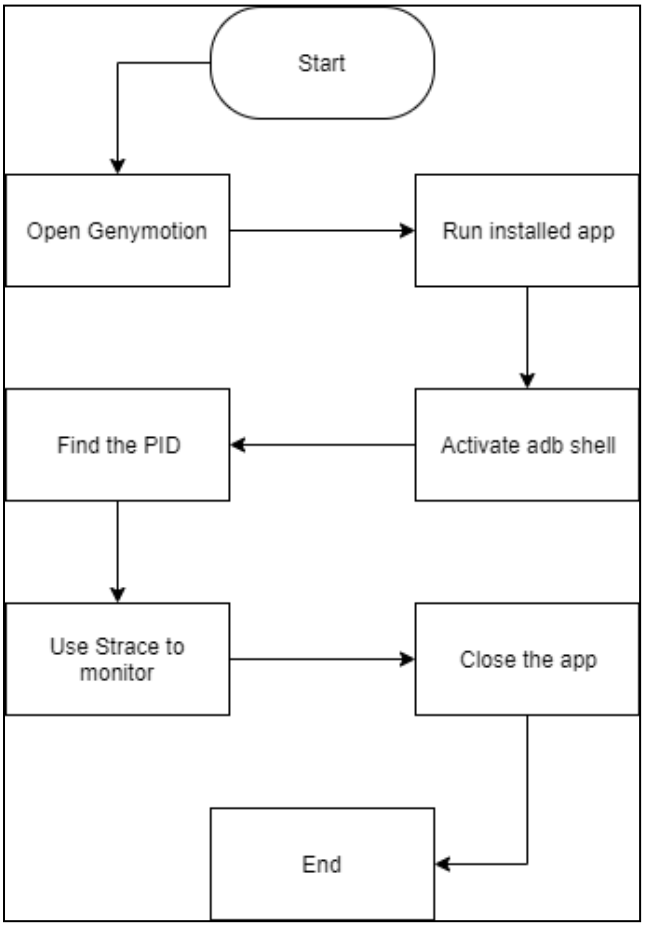
Peneliti mengambil topik ini karena didasari dari beberapa temuan, temuan pertama yakni pada jurnal yang membahas tentang *Malware* di masa depan oleh penelitian yang dilakukan Sapna pada tahun 2019 Dimana pada paper tersebut menemukan adanya perbedaan pada perilaku malware pada tahun 2011 dan 2012 seperti yang dijelaskan pada bab pertama namun pengujian tersebut hanya melibatkan 2 kategori malware dan data yang diteliti adalah data malware yang tergolong lama. Temuan selanjutnya berdasar pada Chakkaravarthy pada tahun 2019 karena didalam nya menyajikan penelitian yang membahas tentang bagaimana malware akan terus berkembang dan menghasilkan ancaman yang lebih berbahaya serta sulitnya melakukan pendeteksian.

2.1 Proses Pengkategorian

Untuk mengetahui kategori malware yang akan dianalisis peniliti menggunakan situs web virustotal untuk mendapatkan kategori tersebut dengan cara memasukkan data yang diperoleh ke virustotal yang selanjutnya akan dideteksi oleh situs web tersebut.

2.2 Analisis dinamis

Guna mengetahui bagaimana cara kerja dari *Malware* yang terdapat pada aplikasi tersebut dilakukan analisis pada saat aplikasi berjalan dengan menganalisa sistem yang dipanggil oleh aplikasi tersebut, Analisis ini akan dilakukan dengan menggunakan tool *strace* adapun proses penelitian disajikan dalam bentuk diagram alir (*Flowchart*) pada Gambar 1.

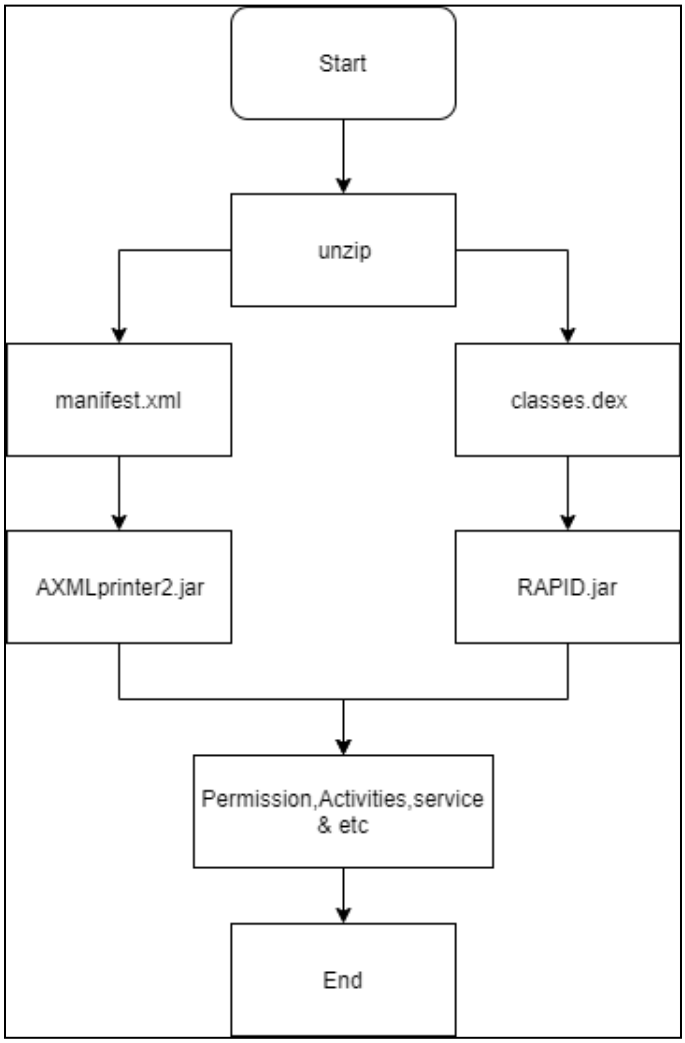


Gambar 1. Alur Analisis Dinamis.

i. Buka emulator android Genymotion dan *install* aplikasi yang akan dianalisis.
ii. Menjalankan aplikasi yang telah di-*install*. Aplikasi akan dijalankan pada emulator guna mengurangi resiko yang tidak diinginkan jika menggunakan device android.
iii. Saat aplikasi telah dijalankan pada emulator selanjutnya mengaktifkan adb shell pada Genymotion dengan mengakses file yang ada di folder genymobile > genymotion > tools > adb.exe dengan menggunakan *Command Prompt.*
iv. Pada tahap selanjutnya setelah menjalankan adb.exe pada CMD dilakukan proses sebagai berikut:
    1. Ketikkan “ps” untuk melihat proses yang sedang berjalan pada android
    2. Cari kolom PID dan pilih PID yang akan di Ketikkan strace –p (PID) –c, dimana “p” sebagai penentu PID dan “c” untuk memantau sistem yang dipanggil oleh *Malware* tersebut
    3. Ketikkan strace –p (PID) –c, dimana “p” sebagai penentu PID dan “c” untuk memantau sistem yang dipanggil oleh *Malware* tersebut.
    4. Untuk mendapatkan hasil maksimal cobalah untuk mengoperasikan aplikasi tersebut agar seluruh sistem yang dipanggil dapat tercatat.
    5. Tutup aplikasi dan data sistem yang dipanggil akan ditampilkan secara keseluruhan di dalam CMD.

2.3 Analisis statis

Setelah melakukan analisis pada sistem yang berjalan dan pemanggilan sistem telah diperoleh selanjutnya memulai proses analisis statis dengan mengekstrak aplikasi tersebut dan menganalisis *source code* dari *Malware* tersebut. Adapun alur penelitian di gambarkan dalam bentuk diagram alir (*Flowchart*) seperti pada Gambar 2.



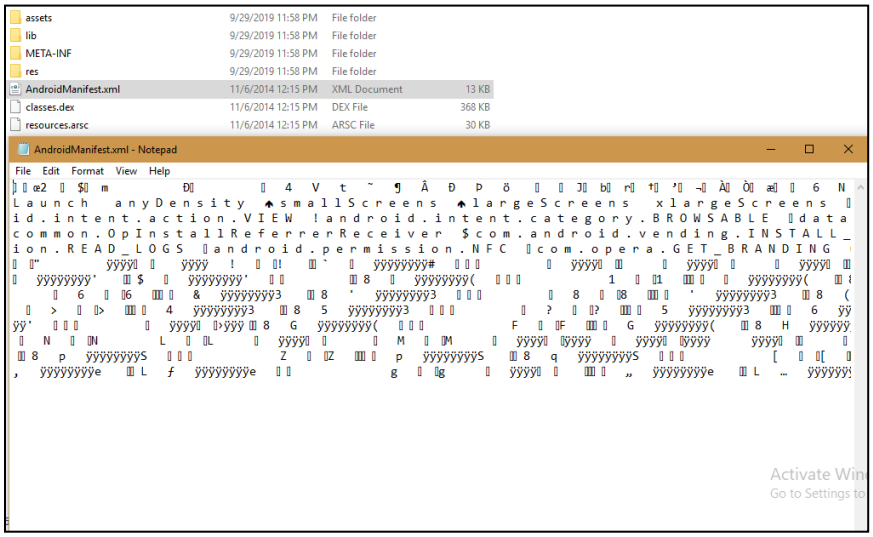
Gambar 2. Alur Analisis Statis

Adapun proses analisis nya dijelaskan sebagai berikut:

i. Setelah mengamati analisis dinamis peneliti mendapatkan beberapa data mengenai sistem yang dipanggil dari *Malware* tersebut, selanjutnya untuk mengetahui mengapa sistem tersebut dipanggil kita perlu menganalisis kode program dari aplikasi tersebut. Hal pertama yang dilakukan adalah mengekstrak aplikasi yang akan menghasilkan beberapa file berikut yakni *manifest.xml, classes.dex, assets, res* dll.

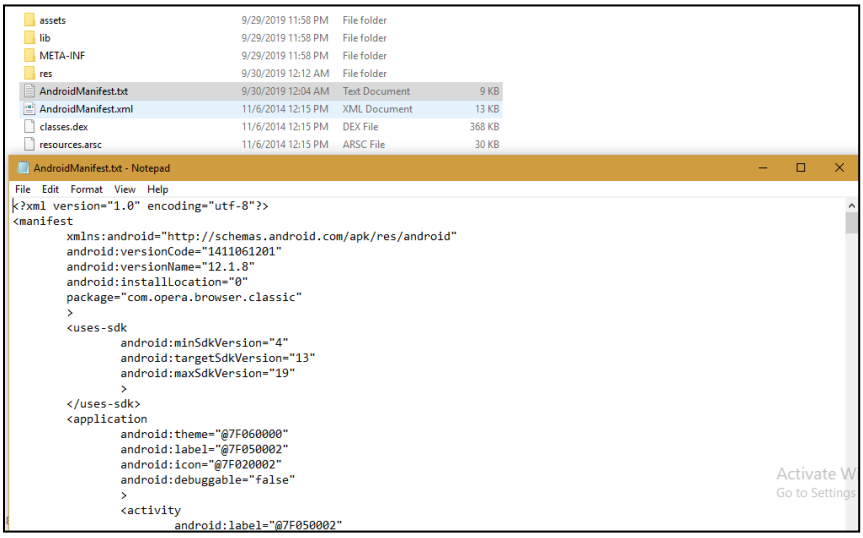
ii. Proses kedua adalah dari file yang telah diperoleh sebelumnya peneliti tidak akan langsung melakukan proses analisa terhadap kode program melainkan peneliti akan membagi 2 proses baru yakni proses mendapatkan *permission, service, uses features* dll serta proses untuk mendapatkan *API calls*. Alasan mengapa proses dibagi menjadi 2 karena untuk menganalisa file .dex biasanya dibutuhkan *Rapid Android Parser jar* untuk memperoleh data *API calls* dan RAPID jar tidak bisa digunakan untuk menganilisa file *manifest.*

iii. Untuk mendapatkan informasi pada file *Manifest.XML* pertama perlu membuat file tersebut menjadi file yang dapat terbaca dengan melakukan proses sebagai berikut :
   a. Ekstrak aplikasi yang akan dieksekusi
   b. Buka *Command Prompt* dan temukan folder yang berisikan aplikasi yang telah diekstrak.
   c. Masuk kedalam folder dan cari file yang akan di eksekusi
   d. Gambar 3 dibawah adalah Tampilan file sebelum dilakukan proses dengan library AXMLprinter.



Gambar 3. File Sebelum Diproses Library AXMLprinter

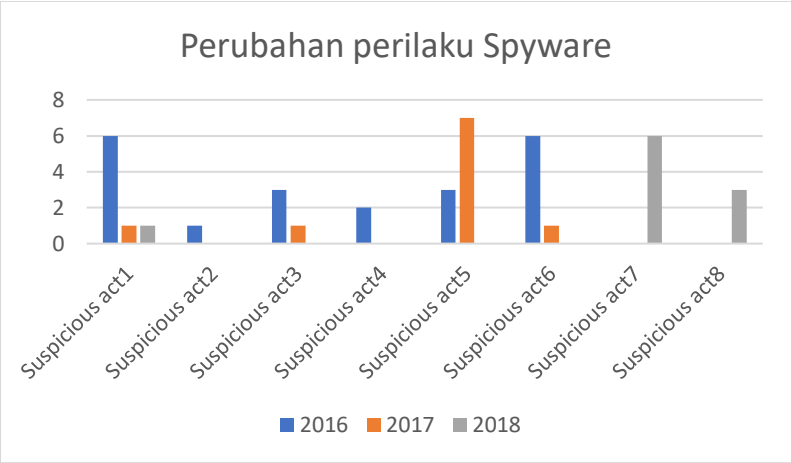
e. Setelah itu ketikkan perintah berikut “java –jar AXMLprinter2.jar file.xml > file.txt
f. Setelah perintah tadi dimasukkan file .xml akan dirubah menjadi file .txt agar data dapat terbaca.
g. Gambar 4 dibawah menunjukkan file setelah proses dengan library.



Gambar 4. File Setelah Diproses Dengan AXMLprinter

iv. Untuk mendapatkan informasi pada file *Classes.DEX* penulis akan menggunakan sebuah program yang dibuat khusus untuk membaca file berekstensi .dex , berikut adalah proses untuk mendapatkan informasi tersebut:
a. Cari file yang akan diekstrak informasinya
b. Pindahkan file tersebut kedalam folder RAPID > SampleAPK
c. Buka *Command Prompt*
d. Masuk kedalam folder RAPID. Pada laptop peneliti folder rapid disimpan pada sistem penyimpanan “E” dan pada folder “Research”
e. Pada *CMD* ketikkan perintah sebagai berikut “java –cp RAPID.jar sample.java”. “sample.java” adalah program yang datang bersamaan dengan library RAPID.jar yang digunakan untuk mengesktrak informasi.
f. Setelahnya masukkan perintah “java –cp .;RAPID.jar sample”
g. Informasi akan langsung ditampilkan pada *CMD* tambahkan perintah “> file.txt” untuk menyimpan file.

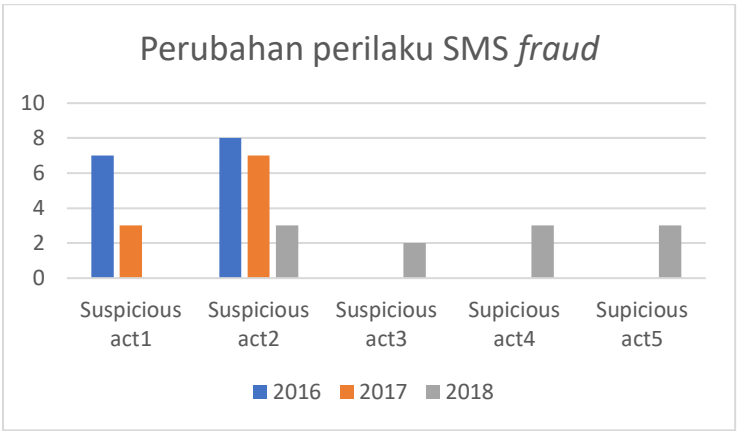
3. Hasil Penelitian dan Pembahasan



Gambar 5. Perubahan perilaku Spyware dari tahun 2016-2018

Gambar 5 menjelaskan tentang perilaku Spyware yang terjadi pada periode tahun 2016-2018 dengan keterangan:

1. Suspicous act1: Send device Information, Network information, Phone data, SD card Data to Remote Server, Contacts
2. Suspicous act2: Send device Information, Installed apps data, Network information, Phone data, SD card Data to Remote Server
3. Suspicous act3: Send device Information, Network information, Phone data, SD card Data to Remote Server
4. Suspicous act4: Send device Information, Network information, Phone data, SD card Data to Remote Server, read users message
5. Suspicous act5: Send device Information, Network information, Phone data, SD card Data to Remote Server, monitoring opened apps, read users message
6. Suspicous act6: Send device Information, Network information, Phone data, SD card Data to Remote Server, intalling other apps, read users message, send message without user knowing
7. Suspicous act7: Send device Information, Network information, Phone data, SD card Data to Remote Server, intalling other apps, read users message, send message without user knowing

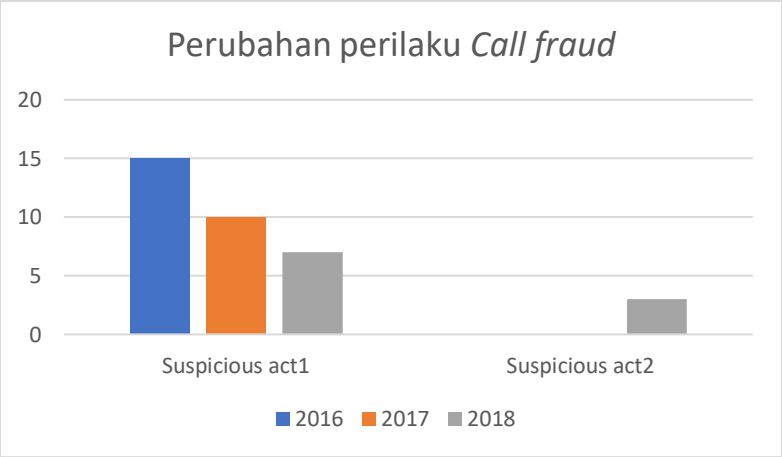


Gambar 6. Perubahan perilaku SMS fraud dari tahun 2016-2018.

Gambar 6 menjelaskan tentang perilaku SMS Fraud yang terjadi pada periode tahun 2016-2018 dengan keterangan:

1. Suspicous act1: Send SMS, Delete SMS, Process SMS, Read SMS

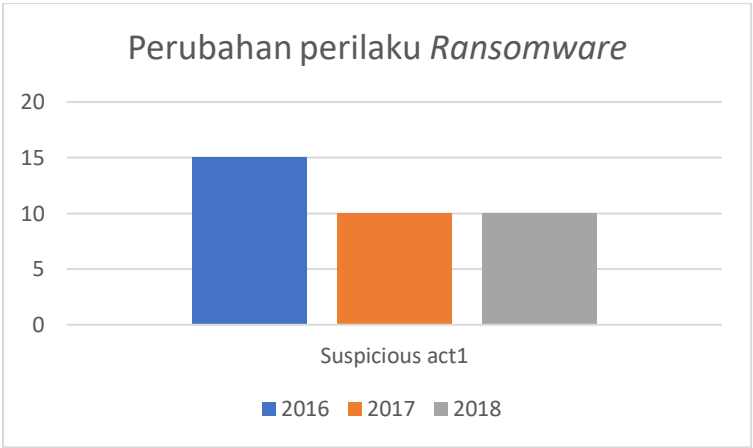
2. Suspicous act2: Send SMS, Delete SMS, Process SMS, Read SMS, Send Device info to remote Server
3. Suspicous act3: Send device Information, Network information, Phone data to Remote Server, read users message, send message without user knowing
4. Suspicous act4: Send device Information, Network information, Phone data, SD card Data to Remote Server, intalling other apps, read users message, send message without user knowing
5. Suspicous act5: Send device Information Network information, Phone data, SD card Data to Remote Server, intalling other apps, read users message, send message without user knowing, making a call



Gambar 7. Perubahan perilaku Call fraud dari tahun 2016-2018

Gambar 7 menjelaskan tentang perilaku Call Fraud yang terjadi pada periode tahun 2016-2018 dengan keterangan:

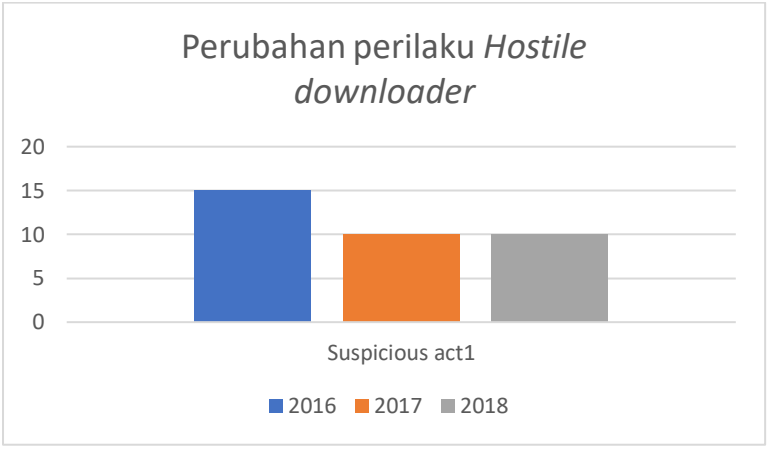
1. Suspicious act1: Send device info, making call, record outgoing call, dial phone number,terminate call,check user contact
2. Suspicious act2: Send device info, making call, record outgoing call, dial phone number,terminate call,check user contact,read user message,send sms



Gambar 8. Perubahan perilaku Ransomware dari tahun 2016-2018

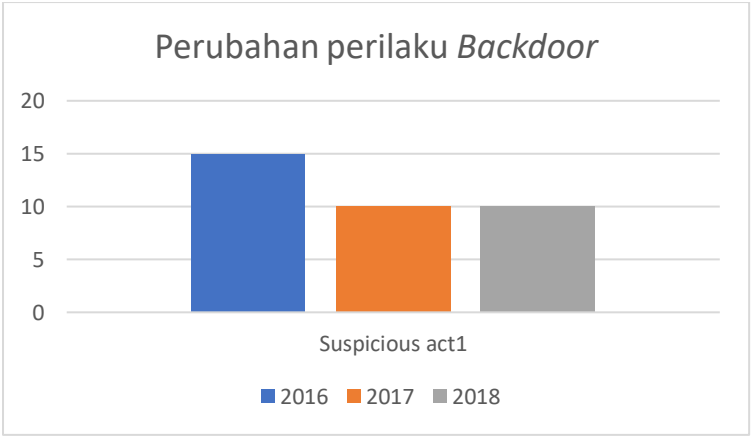
Gambar 8 menjelaskan tentang perilaku Ransomware yang terjadi pada periode tahun 2016-2018 dengan keterangan:

1. Suspicious act1: Send device info, send device data, install other apps, download other apps, start camera, send SMS, read SMS, delete SMS, send network information, check user activity, make a call, record everything related to audio



Gambar 9. Perubahan perilaku Hostile downloader dari tahun 2016-2018

Gambar 9 menjelaskan tentang perilaku Ransomware yang terjadi pada periode tahun 2016-2018 dengan keterangan Suspicious act1: Install other apps



Gambar 10. Perubahan perilaku Backdoor dari tahun 2016-2018

Gambar 10 menjelaskan tentang perilaku Backdoor yang terjadi pada periode tahun 2016-2018 dengan keterangan: Suspicious act1: Send device info,send device data,install other apps,download other apps,start camera,send SMS,read SMS,delete SMS,send network information,check user activity,make a call,record everything related to audio

4.1 Pembahasan

4.1.1 Perubahan yang terjadi

Setelah meneliti dan melakukan analisis ditemukan bahwa pada beberapa kategori malware telah mengalami perubahan yang signifikan dan beberapa yang menunjukkan segelintir perubahan serta dari beberapa kategori malware yang diteliti hasil menunjukan bahwa ada kemungkinan bahwa malware tersebut telah bercampur menjadi satu berikut penjelasan nya.

a) Spyware

Pada malware kategori *spyware* ditemukan telah adanya perbedaan dari data yang diteliti pada tahun 2016 dengan data terbaru, dimana semua data terbaru menunjukan perubahan perilaku dari data tahun 2016 yang mana pada data terbaru menunjukkan bahwa *spyware* yang awalnya hanya berguna untuk memata – matai dan mencuri akun sekarang sudah dapat melakukan aktivitas seperti mengirim SMS ,membaca log panggilan, hingga menginstall aplikasi lain nya tanpa disadari oleh pengguna.

b) SMS fraud

Berbeda dengan *spyware* yang terjadi pada SMS *fraud* adalah kebalikan dari *spyware* itu sendiri dimana data awal menunjukkan bahwa SMS fraud digunakan hanya untuk memantau SMS yang masuk, membaca, dan mengirim pesan tanpa diketahui pengguna sekarang SMS

fraud telah dapat melakukan apa yang dapat dilakukan oleh *spyware* meski tidak semua data yang diteliti memperlihatkan hasil perubahan yang besar namun diantaranya sudah dapat melakukan pengiriman informasi yang ada pada perangkat kepada pembuat malware.

c) Call fraud

Pada kasus *Call fraud* tidak terjadi begitu banyak perubahan karena dari data yang diteliti tidak sampai separuh dari data yang menunjukkan perubahan namun dari data yang diteliti perubahan terlihat dari adanya aksi serupa dengan SMS *fraud* yaiut mengirim dan membaca SMS.

d) Ransomware

Seperti kasus pada kategori sebelumnya pada ransomware terlihat tidak ada perubahan sama sekali dimana semua data yang diteliti menunjukkan hasil yang sama yang berarti tidak ada perubahan yang terjadi pada kategori tersebut.

e) Hostile downloader

Pada hostile downloader peneliti tidak menuliskan perilaku lain nya selain hanya menginstall sebuah aplikasi karena pada dasarnya kegunaan dari malware tersebut adalah hanya untuk menginstall aplikasi lain namun untuk mengetahui apakah aplikasi yang di install berbahaya atau tidak tidak dapat diketahui.

f) Backdoor

Kasus serupa seperti *Ransomware* terjadi pada backdoor dimana tidak terjadi perubahan apapun dari data lama hingga data baru yang diteliti.

Dari 6 kategori malware yang diteliti terlihat bahwa 3 diantaranya mengalami perubahan sementara 3 lain nya tidak, namun hasil penelitian juga mengungkap bahwa dari 4 kategori malware yang dibahas beberapa data didalamnya memiliki sebuah kesamaan didalamnya yang menghasilkan sebuah kemungkinan bahwa telah muncul sebuah kategori baru berdasarkan data tersebut. Keempat kategori tersebut adalah *Spyware,* SMS *fraud, call fraud,* dan *hostile downloader* dimana beberapa data terbaru menunjukkan bahwa *Spyware* dapat melakukan pengiriman sms, menelpon, dan menginstall sebuah aplikasi begitupula yang terjadi pada SMS *fraud* yang telah bisa meminta informasi yang ada pada perangkat korban dan melakukan panggilan. Sedangkan pada *call fraud* data menunjukkan bahwa malware tersebut telah dapat melakukan hal yang sama seperti yang dilakukan oleh kategori SMS *fraud.*

5. Kesimpulan

Kesimpulan dari penelitian ini, untuk memajukan pengembangan terhadap sistem deteksi antivirus adakalanya peneliti harus melihat dan membandingkan data hasil penelitian terbaru dengan penelitian sebelumnya alasannya adalah jika peneliti bisa mengetahui sedikit demi sedikit celah perubahan yang terjadi maka ada kemungkinan untuk peneliti mengetahui gerak dari *Malware* yang akan datang dan dapat membuat tindakan pencegahan sehingga tidak terjadi kasus yang dapat merugikan masyarakat. Kedepan nya jika penulis memiliki kesempatan maka penulis ingin melanjutkan penelitian kejenjang dimana penulis bisa mengetahui sedikit tentang prediksi dan antisipasi terhadap malware yang akan datang.

Referensi

[1] F. Tong and Z. Yan, “A hybrid approach of mobile malware detection in Android,” *J. Parallel Distrib. Comput.*, vol. 103, pp. 22–31, 2017.

[2] M. K. Alzaylaee, S. Y. Yerima, and S. Sezer, “DynaLog: An automated dynamic analysis framework for characterizing android applications,” *2016 Int. Conf. Cyber Secur. Prot. Digit. Serv. Cyber Secur. 2016*, 2016.

[3] J. B. Shukla, G. Singh, P. Shukla, and A. Tripathi, “Modeling and analysis of the effects of antivirus software on an infected computer network,” *Appl. Math. Comput.*, vol. 227, pp. 11–18, 2014.

[4] Monika, P. Zavarsky, and D. Lindskog, “Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization,” *Procedia Comput. Sci.*, vol. 94, pp. 465–472, 2016.

[5] I. Martín, J. A. Hernández, and S. de los Santos, “Machine-Learning based analysis and classification of Android malware signatures,” *Futur. Gener. Comput. Syst.*, 2019.

[6] Y. Zhang, W. Ren, T. Zhu, and Y. Ren, “SaaS: A situational awareness and analysis system for massive android malware detection,” *Futur. Gener. Comput. Syst.*, vol. 95, pp. 548–559, 2019.

[7] S. S. Chakkaravarthy, D. Sangeetha, and V. Vaidehi, “A Survey on malware analysis and mitigation techniques,” *Comput. Sci. Rev.*, vol. 32, pp. 1–23, 2019.
[8] S. Malik and K. Khatter, “System Call Analysis of Android Malware Families,” vol. 9, no. June, 2016.
[9] D. Saif, S. M. El-Gokhy, and E. Sallam, “Deep Belief Networks-based framework for malware detection in Android systems,” *Alexandria Eng. J.*, vol. 57, no. 4, pp. 4049–4057, 2018.