Analisis *Malware Ahmyth* pada Platform Android Menggunakan Metode *Reverse Engineering*

Nur Widiyasono[1], Husni Mubarok[2], Agung Fatwa MF[3]
[1,2,3]Informatika, Fakultas Teknik, Universitas Siliwangi, Tasikmalaya
E-mail: *[1]*nur.windiyasono@unsil.ac.id*, [2]husni.mubarok@unsil.ac.id,
[3] agung.fatwa@student.unsil.ac.id

Abstrak – *Android merupakan sistem operasi yang paling banyak digunakan didunia dengan persentase sebesar 74.82% pada pangsa pasar sistem oeprasi android. Fakta ini membuat para pengembang malicious software (malware) menjadikan pengguna telepon seluler dengan sistem operasi android sebagai target utama serangan malware. Penyerang dapat mengubah kode aplikasi dengan memasukan malicious code, mengemas ulang aplikasi dan mempublikasikan aplikasi tersebut di pasar aplikasi android. Penelitian ini bertujuan untuk mengetahui cara kerja suatu malware yang telah disisipkan pada aplikasi android dengan menggunakan analisis dinamis dan mengekstrak perijinan berbahaya yang digunakan malware ahmyth dengan menggunakan teknik reverse engineering. Hasil analisis menunjukan bahwa malware ahmyth akan menjalankan servicenya setelah perangkat melakukan restart dan menunggu perintah dari C&C server untuk melakukan tindakan tertentu pada perangkat yang terinfeksi.*

Kata Kunci *— Ahmyth, Analisis, Android, Engineering, Reverse*

Abstract – *Android is the most widely used operating system in the world with a percentage of 74.82% in the Android operating system market share. This fact makes malicious software (malware) developers make mobile phone users with the Android operating system the main target for malware attacks. Attackers can change the application code by entering malicious code, repackaging the application, and publishing the application on the android application market. This study aims to find out how the malware that has been inserted into the android application works by using dynamic analysis and extracting the dangerous licenses used by the ahmyth malware by using reverse engineering techniques. The results of the analysis show that the ahmyth malware will run its service after the device restarts and waits for commands from the C&C server to perform certain actions on the infected device.*

Keywords *— Ahmyth, Analysis, Android, Engineering, Reverse*

1. PENDAHULUAN

Android merupakan system operasi mobile paling banyak digunakan saat ini diseluruh dunia, sebanyak 74.82% pangsa pasar system operasi telepon pintar dikuasai oleh android.(Statcounter, 2018). Fakta ini membuat para pengembang malicious software atau malware menjadikan pengguna telepon seluler dengan sistem operasi android sebagai target utama serangan malware.

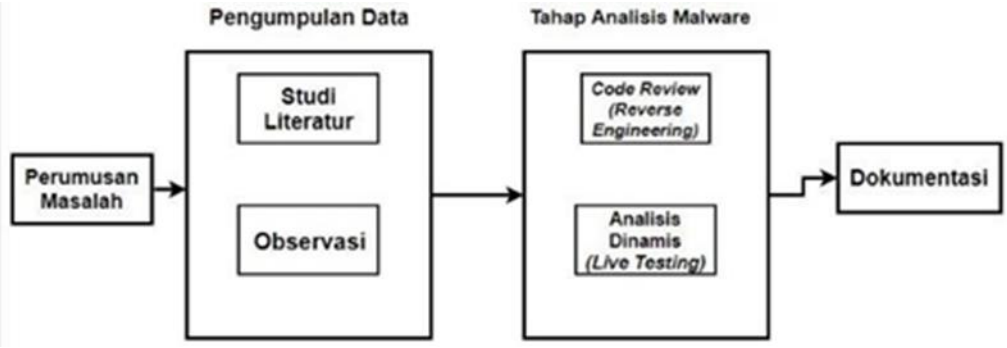
Statistik menunjukan adanya peningkatan jumlah mobile malware sejak tahun 2017. Terdapat peningkatan sebanyak 70% antara tahun 2016 sampai tahun 2017, dan peningkatan jenis mobile malware baru sebanyak 8.33 % pada tahun 2017, dari jumlah tahun 2016 dengan jumlah sebanyak 2.400.000. (McAfee Lab, 2018). Tingginya pertumbuhan mobile malware masih banyak aplikasi berbahaya yang bahkan di temukan pada android market, hal ini menjadi sangat berbahaya bagi pengguna perangkat android, karena pengguna berpeluang mendownload aplikasi android yang sudah disusupi kode malware didalamnya. Penyerang dapat menarik pengguna untuk mengunduh perangkat lunak yang telah ditambahkan kode malware dengan cara mengemas ulang aplikasi dengan menggunakan tools reverse engineering. Penyerang mengubah kode aplikasi untuk memasukan kode jahat, mengemas ulang aplikasi dan mempublikasikan aplikasi tersebut di pasar

aplikasi android, pengguna pada umumnya tidak dapat membedakan antara aplikasi resmi dan aplikasi yang telah disusupi malware. (Rubayyi Alghamdi, 2015).

Penelitian ini menggunakan teknik reverse engineering dan analisis dinamis dengan tujuan untuk mengetahui cara kerja dari malware ahmyth. Reverse engineering merupakan proses untuk menemukan dan mengetahui cara kerja sebuah aplikasi dengan mempelajari cara operasi, struktur dan fungsi dari aplikasi tersebut. (Vibha Manjunath, 2012) . Software yang digunakan untuk melakukan reverse engineering diantaranya, ApkTool, Dex2Jar, JD-GUI, Notepad++, dan Android SDK.

Kemampuan analisis diperlukan untuk melakukan analisa malware ahmyth dengan teknik reverse engineering dan dynamic analysist terhadap malware yang ada dengan tujuan untuk menjadi acuan dan meningkatkan kesadaran bagi pengguna perangkat mobile sehingga dapat mencegah atau mengurangi tingkat pengrusakan dan pencurian data yang dapat merugikan pengguna perangkat mobile.

2. METODE PENELITIAN



Gambar 1. Alur Penelitian

1) Perumusan Masalah

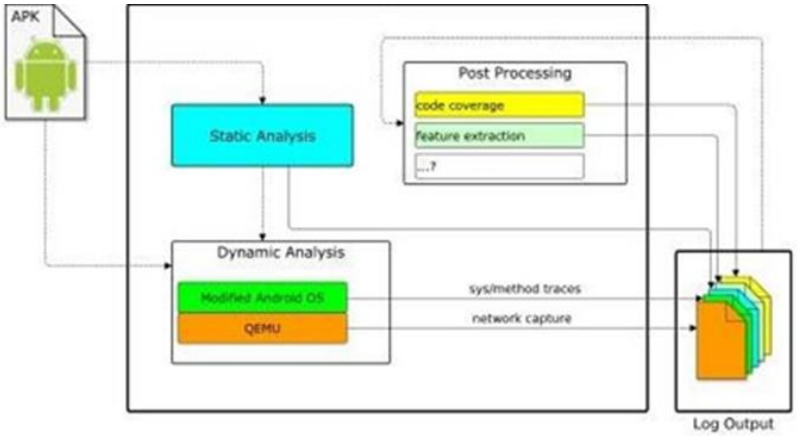
Proses perumusan masalah didapat dari kejadian meningkatnya perkembangan malware dengan platform smartphone di dunia, terjadi peningkatan sebesar 70% pada tahun 2017, maka dari itu penelitian ini melakukan Analisa terhadap salah satu malware platform android yaitu malware ahmyth dengan tipe spyware malware.

2) Pengumpulan Data

Metode pengumpulan data dilakukan dengan mengidentifikasi dan membuat alur perancangan yang akan dilaksanakan, agar proses pencarian data tidak terjadi penyimpangan dalam mengemukakan suatu tujuan yang ingin dicapai.

3) Tahap Analisis Malware

Metode analisis malware yang digunakan pada penelitian ini menggunakan metode analisis statis dan analisis dinamis. Tahapan analisis malware dengan menggunakan kedua metode tersebut secara garis besar diilustrasikan seperti pada gambar 2.

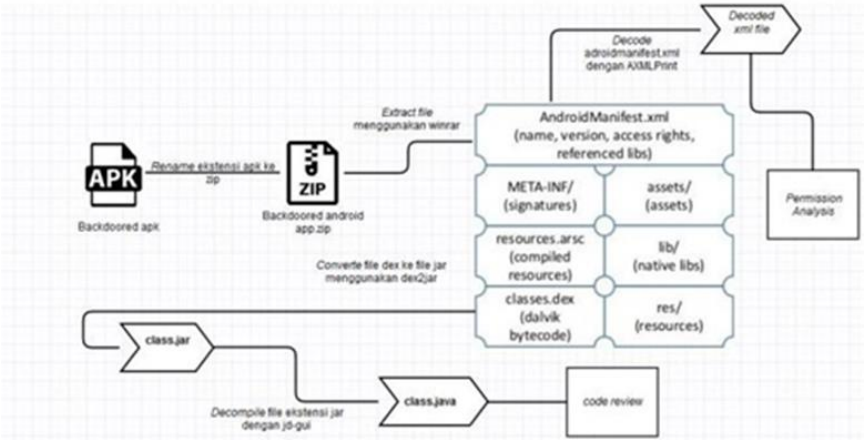


Gambar. 2 Tahapan Metode Analisis Malware Merujuk Vaan Der Ven (2013).

3. HASIL DAN PEMBAHASAN

A. Static Analysis

Analisis statis ini menggunakan teknik reverse engineering untuk mendapatkan java source code dari aplikasi android yang telah terinfeksi oleh malware ahmyth untuk kemudian source code tersebut dianalisis, secara garis besar tahapan reverse engineering yang akan dilakukan adalah sebagai berikut :



Gambar. 3 Alur reverse engineering file apk

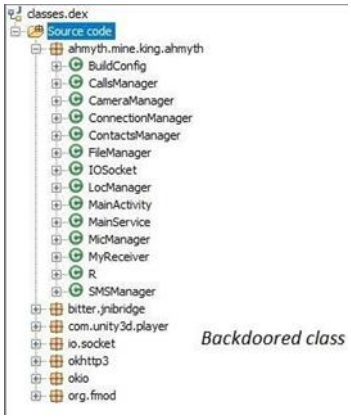
Ekstensi file apk yang dijadikan sampel dirubah ke ekstensi zip dengan tujuan melakukan ekstraksi file-file yang terkompres pada file yang dijadikan sampel tersebut, akan muncul beberapa file hasil ekstraksi diantaranya adalah AndroidManifest. File xml bytecode ini membutuhkan proses konversi dengan menggunakan tool AXMLPrinter. Perijinan yang didapat dari hasil decode, akan dikelompokan pada dua level keamanan untuk mengetahui potensi kerusakan yang akan ditimbulkan oleh aplikasi android yang telah terinfeksi malware ahmyth tersebut.

Tabel 1. Analisis Perijinan Yang Digunakan Ahmyht

Permission	**Status**	**Keterangan**
android. permission. WAKE_LOC K	*Normal Permissi on*	*Memungkinkan aplikasi untuk menggunakan layanan PowerManager untuk mempertahankan prosessor agar tetap dalam keadaan standby*
android. permission. CAMERA	*Dangero us Permission*	*layanan yang berhubungan dengan akses terhadap kamera atau untuk menangkap gambar/video dari perangkat android*
android.permission. WRITE_ EXTERNAL STORAGE	*Dangerous Permission*	*file pada perangkat external seperti sd card*

android. permission. INTERNET	*Normal Permission*	*mengakses network services, memungkinkan malware ahmyth untuk berkomunikasi dengan C&C (command and control)server.*
android. permission. ACCESS_ NETWORK_ STATE	*Normal Permission*	*memeriksa status internet dan mengakses connectivity manager yang berguna untuk memonitor koneksi jaringan*
android.permission. READ_SMS	*Dangerous Permission*	*Perijinan ini dibutuhkan ketika aplikasi akan melakukan aksi listen dan read pesan SMS, perijinan ini digunakan secara luas pada aplikasi yang membutuhkan fungsi OTP (One Time Password)*
android.permission. SEND_SMS	*Dangerous Permission*	*memungkinkan aplikasi mengakses sms manager dan mengirimkan sms rahasia kepada nomor yang dituju*
android.permission.RECEI VE_BOOT_COMPLETED	*Normal Permission*	*memungkinkan malware ahmyth untuk berjalan secara otomatis pada saat perangkat terpasang melakukan restart, hasilnya pada saat boot malware ahmyth akan berjalan pada background process*
android.permission.READ_ PHONE_STATE	*Dangerous Permission*	*mengakses informasi status telepon seluler, seperti nomor telepon yang ada pada perangat, informasi jaringan seluler yang sedang digunakan, dan status panggilan masuk.*
android.permission.READ_ EXTERNAL_STORAGE	*Dangero us Permission*	*Menijinkan aplikasi untuk mengakses penyimpanan external seperti kartu sd.*
android.perm ission.READ_ CALL_LOG	*Dangero us Permission*	*Mengijinkan aplikasi untuk mengakses riwayat panggilan.*
android.perm ission.RECO RD_AUDIO	*Dangerous Permission*	*memiliki fungsi untuk merekam audio secara otomatis tanpa diketahui oleh pengguna.*
android.perm ission.MODI FY_AUDIO_ SETTINGS	*Normal Permission*	*mengakses dan memodifikasi pengaturan audio.*
android.perm ission.ACCE SS_FINE_LOCATION	*Dangerous Permission*	*mengetahui posisi perangkat yang telah terinfeksi pada map*
android.perm ission.READ _CONTACTS	*Dangerous Permission*	*mengirim informasi kontak dari perangkat yang telah terinfeksi kepada C&C server.*

Class.dex merupakan file executable yang dapat berjalan pada dalvik virtual machine, didalam file ini terdapat class yang dibutuhkan oleh aplikasi pada saat runtime, teknik reverse engineering dibutuhkan pada file class.dex agar class menjadi kode dengan bahasa java, dilakukan proses convert pada dex file untuk mengubah dalvik executable ke file format jar menggunakan dex2jar, langkah terkahir decompile file jar dengan menggunakan jd-gui atau jadx agar struktur class java dan source code java dari aplikasi dapat dianalisis.



Gambar. 3 Package malware ahmyth

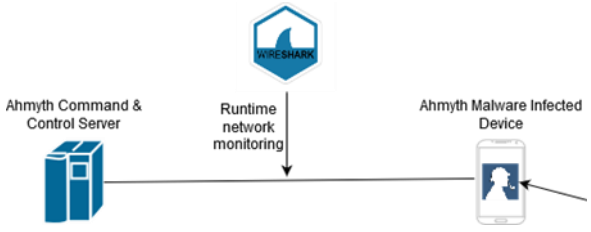
Hasil decompile file class.dex, terlihat ada penambahan package dengan nama ahmyth.mine.king.ahmyth paket ini memuat class yang digunakan malware ahmyth untuk menjalankan service yang berhubungan dengan permission yang telah didefinisikan pada file androidmanifest.xml.

Tabel 2. Class Pemanggil Fungsi API

API	Landroid/hardware/Camera;->open
Caller Code	Lahmyth/mine/king/ahmyth/**CameraMana ger**;->startUp(I)V
Deskripsi	Membuka akses pada kamera
API	Landroid/hardware/Camera;->takePicture
Caller Code	Lahmyth/mine/king/ahmyth/**CameraMana ger**;->startUp(I)V
Deskripsi	Kelas *camera manager* dapat melakukan penangkapan gambar melalui kemera tanpa sepengetahuan pengguna.
API	Landroid/location/LocationManager;->getL astKnownLocation
Caller Code	Lahmyth/mine/king/ahmyth/**LocManager**;->getLocation()Landroid/location/Location;
Deskripsi	Kelas LocManager memungkinkan *malware* ahmyth untuk melakukan deteksi lokasi perangkat yang terinfeksi.
API	Landroid/telephony/SmsManager;->sendTe xtMessage
Caller Code	Lahmyth/mine/king/ahmyth/SMSManager;->sendSMS
Deskripsi	Kelas smsManager memungkinkan *malware* ahmyth untuk mengirim pesan sms ke nomor yang dituju tanpa sepengetahuan pengguna.
API	Ljava/net/URL;->openConnection
Caller Code	Lio/socket/engineio/client/transports/Polling XHR$Request;->create()V
Deskripsi	Kelas PollingXHR dapat melakukan koneksi ke C&C server untuk menerima perintah atau mengirim hasil *spying* pada perangkat yang terinfeksi.
API	Landroid/hardware/Camera;->open

B. Dynamic Analysist

Proses pengujian analisis dinamis terhadap malware ahmyth dilakukan pada lingkungan virtual menggunakan genymotion, jaringan local (LAN) dibutuhkan a gar malware ahmyth dapat berkomunikasi dengan C&C server.



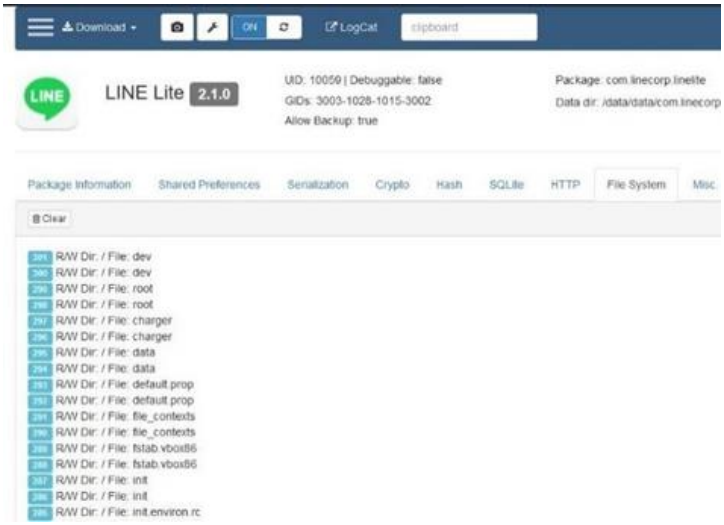
Gambar. 4 Dynamic analysist lab setup

Proses pengujian metode analisis dinamis menggunakan satu host komputer dengan alamat IP 192.168.100.16 yang bertujuan untuk mengontrol tindakan yang akan dilakukan malware ahmyth terhadap perangkat yang terinfeksi. Perangkat android yang dipakai adalah perangkat dengan sistem operasi android 4.4.2, malware yang menginfeksi perangkat ini menggunakan alamat 192.168.10.12

dengan port 6596 untuk berkomunikasi dan mendapatkan perintah dengan command and control server (C&C server).

1) Inspeckage

Proses menganalisa service yang dijalankan malware ahmyth saat dalam keadaan runtime dilakukan dengan menggunakan aplikasi inspeckage dan xposed, inspeckage akan melakukan hook pada service ahmyth dan merekam apa yang dilakukan malware ahmyth terhadap sistem pada saat runtime.



Gambar. 5 Riwayat akses malware ahmyth terhadap direktori system

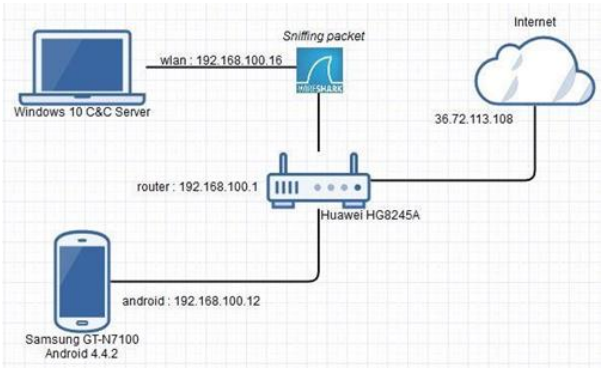
Proses monitoring aktifitas akses malware ahmyth terhadap direktori sistem perangkat android yang terinfeksi, inspeckage merekam prilaku malware ahmyth ketika mengakses direktori root perangkat terinfeksi, terlihat pada log histori R/W Dir: / File: dev, R/W Dir: / File: sdcard , yang artinya malware ahmyth mengakses direktori / (root) dan pada direktori root terdapat sub direktori dev dan sdcard.

Tabel 3. Log Service Malware Ahmyth

1	`registerReceiver: Actions: android.intent.action.SCREEN_ON,android.intent.action.SCREEN_OFF,android.intent.action.USER_PRESENT`
2	`startService: Intent { cmp=com.linecorp.linelite/ahmyth.mine.king.ahmyth.MainService }`
3	`startService: Intent { cmp=com.linecorp.linelite/ahmyth.mine.king.ahmyth.MainService }`
4	`startActivity: Intent { flg=0x24000000 cmp=com.linecorp.linelite/.ui.android.register.RegisterFirstActivity }`

Ketika aplikasi line dijalankan malware ahmyth akan melakukan running service dengan perintah startService dan menjalankan intent {cmp=com.linecorp.linelite/ahmyth.mine.king.ahmyth.MainService}, class file mainservice dibutuhkan agar malware ahmyth dapat menjalankan fungsinya di background service, ketika service nya melalui tahap onDestroy maka malware ahmyth tidak dapat menghubungi C&C server karena service telah dihentikan.

2) Network Analysist



Gambar. 6 Topologi jaringan untuk proses capture paket

Topologi ini memisahkan perangkat C&C server dengan perangkat korban malware ahmyth, C&C server menggunakan ip 192.168.100.16 dan perangkat korban menggunakan ip 192.168.100.12, kedua perangkat tersebut berada pada segmen jaringan yang sama agar tidak memerlukan dns saat malware ahmyth menginisialisasi koneksi kepada C&C server.

Tabel 4. Log Service Malware Ahmyth

Source	***Destination***	***Protocol***	***Info***
MurataMa_ 43:fc:67	Broadcast	ARP	Who has 192.168.100.16? Tell 192.168.100.12
MS-NLB-PhysServer 03_82:e3:ab:5f	MurataMa_4 3:fc:67	ARP	192.168.100.16 is at 02:03:82:e3:ab:5f
192.168.100.12	192.168.100.16	TCP	34541 → 6596 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=92197846 TSecr=0 WS=2
192.168.100.16	192.168.100.12	TCP	6596 → 34541 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.100.12	192.168.100.16	TCP	34541 → 6596 [RST] Seq=1 Win=0 Len=0
MS-NLB-PhysServer-03_82:e3:ab:5f	MurataMa_4 3:fc:67	ARP	Who has 192.168.100.12? Tell 192.168.100.16
MurataMa_ 43:fc:67	MS-NLB-PhysServer-03_82:e3:ab: 5f	ARP	192.168.100.12 is at 20:02:af:43:fc:67
192.168.100.12	192.168.100.16	TCP	35131 → 6596 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=92198854 TSecr=0 WS=2
192.168.100.16	192.168.100.12	TCP	6596 →35131 [SYN,ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
192.168.100.12	192.168.100.16	TCP	35131 → 6596 [ACK] Seq=1Ack=1 Win=14600 Len=0
192.168.100.12	192.168.100.16	HTTP	GET /socket.io/?EIO=3&id=f8c13 d335ece2c18&model=GT-N7100&manf=samsung&tran sport=polling&release=4.4.2 HTTP/1.1
192.168.100.16	192.168.100.12	HTTP	HTTP/1.1 200 OK (application/octet-stream)

Perangkat android yang terinfeksi dengan ip 192.168.100.12 mengirimkan sebuah broadcast kepada jaringan untuk mengetahui alamat mac dari ip 192.168.100.16 yang merupakan

alamat C&C server, saat proses broadcast selesai server dengan alamat ip 192.168.100.16 akan membalas pesan broadcast bahwa ip tersebut memiliki alamat mac 02:03:82:e3:ab:5f, kemudia dari sisi C&C server melakukan hal yang sama kepada perangkat android yang terinfeksi sehingga kedua perangkat tersebut dapat terhubung.

Tabel 5..Packet Berisi Call Log

Src	192.168.100.12
Dst	192.168.100.16
Protocol	WebSocket
Line-based text data ["x0000cl",{"callsList":[{"type":3,"phoneNo":"+62812235706 65","duration":"0","name":"Dicky A"},{"type":1,"phoneNo":"+6281223570665","duration":"18" ,"name":"Dicky A"},{"type":2,"phoneNo":"081223570665","duration":"13","name":"Dicky A"}	
Hasil menunjukan bahwa perangkat yang terinfeksi malware ahmyth mengirimkan riwayat panggilan telepon kepada server dengan alamat ip 192.168.100.16, dalam paket yang ditangkap terdapat informasi nomor telepon, nama kontak penelepon, dan durasi lama panggilan, paket ini dikirim menggunakan protocol websocket yang sebelumnya telah melalui proses request dan accept antara C&C server dan client ahmyth.	

Tabel 6.Packet Berisi Call Log

Src	192.168.100.12
Dst	192.168.100.16
Protocol	WebSocket
Line-based text data 42["x0000sm",{"s msList":[{"phone No":"TCASH Info" ,"msg":"Kamu pun ya SALDO BONUS, tsel.me\/mngbyk1 "},{"phoneNo":"+ 6281323257928"," msg":"Assalamualaikum.."}	
packet yang ditangkap dengan menggunakan wireshark menemukan bahwa *malware ahmyth* dengan ip 192.168.100.12 mengirimkan informasi pesan masuk kepada C&C server menggunakan protocol websocket, informasi yang dikirim berupa nomor telepon yang mengirim pesan, isi pesan yang diterima oleh perangkat *smartphone*.	

Tabel 7. Packet Berisi Call Log

Src	192.168.100.16
Dst	192.168.100.12
Protocol	WebSocket
Line-based text data 42["order",{"order":"x0000lm"}]	
Src	192.168.100.12
Dst	192.168.100.16
Protocol	WebSocket
Line-based text data 42["x0000lm",{"enable":true,"lng":108.1438904,"lat":- 7.1522285}]	
Menunjukan hasil bahwa C&C server dengan ip address 192.168.100.16 mengirim perintah “order”,{“order”:”x00001m”} kepada perangkat client *malware* dengan alamat ip 192.168.100.12, perintah tersebut berarti *malware* ahmyth mengirimkan perintah kepada client ahmyth untuk mengirimkan kordinat lantitude dan longitude kepada C&C. Client ahmyth dengan ip 192.168.100.12 akan menerima perintah dari C&C server dan akan mengirimkan infromasi sesuai perintah ["x0000lm",{"enable":true,"lng":108.1438904,"lat":-7.1522285}], pesan “enable” berarti layanan gps pada perangkat yang terinfeksi dinyalakan, informasi ,"lng":108.1438904,"lat":-7.1522285 berarti posisi dari perangkat android berada pada garis lintang 108.1438904 dan garis bujur -7.1522285.	

Cara kerja malware ahmyth diantaranya :

- Setelah berhasil dipasang pada perangkat android, malware ahmyth membutuhkan system reboot untuk menjalankan service nya, perijinan receive_reboot_complete memungkinkan malware ahmyth untuk auto-run pada proses booting.
- Selesai menjalankan service, malware ahmyth akan mencari alamat C&C server dengan menggunakan broadcast ARP.

- Malware ahmyth akan mengirim informasi perangkat yang terinfeksi kepada C&C server sesaat setelah alamat ip dan mac address C&C server ditemukan dan saling terhubung dengan C&C server.
- Malware ahmyth akan masuk dalam kondisi standby menunggu perintah dari C&C server, ketika perintah dari C&C server diterima oleh client ahmyth, malware ahmyth mulai menjalankan fungsi sesuai dengan perintah dari C&C server dan mengirim informasi yang diminta kepada C&C server.

1) Karakteristik malwareahmyth

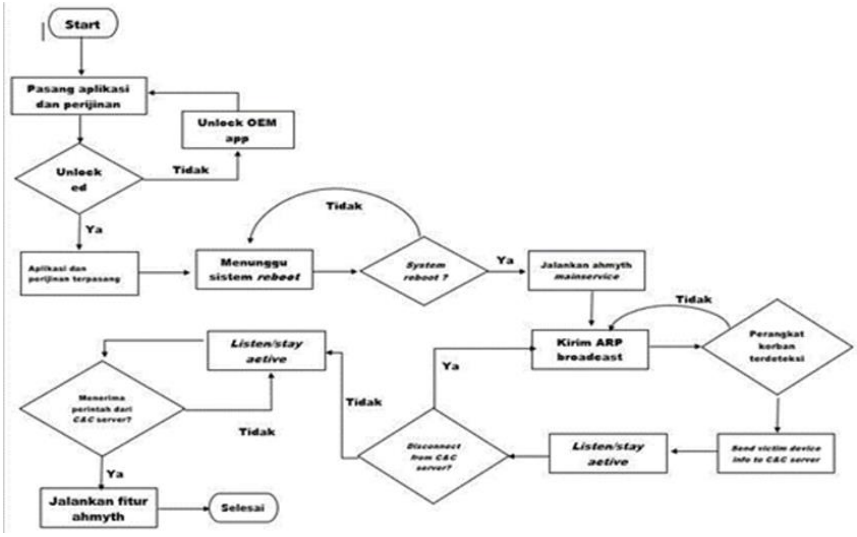
Karakter yang dimiliki oleh malware ahmyth adalah sebagai berikut :

- Memiliki fitur auto reconnect server
- Memiliki fitur wakelock
- Dapat menjalankan service secara otomatis
- Hak akses informasi perangkat korban
- Dapat melakukan remote sms kepada nomor tujuan sesuai permintaan C&C server.
- Dapat melakukan remote akses kepada direktori external dan internal yang ada diperangkat smartphone.
- Dapat melakukan download file
- Memiliki fitur audio recording, Tracking GPS, akses contact list, akses call log, akses kotak masuk pesan sms, stealth camera.

2) Pencegahan malware ahmyth

Pencegahan yang dapat dilakukan untuk melindungi perangkat smartphone dari malware ahmyth secara umum:

- Selalu update versi sistem operasi android
- Tidak mendownload aplikasi dari penyedia yang tidak terpercaya
- Disable fitur install from unknown resource yang terdapat di developer option.
- Install antivirus khusus perangkat android
- Gunakan fitur screen lock pada perangkat android, untuk memastikan perangkat aman dari pemasangan malware secara manual.



Gambar. 7 Ahmyth malware workflow

4. SIMPULAN

Berdasarkan hasil analisis malware ahmyth menggunakan metode statis dan dinamis pada perangkat dengan sistem operasi android 4.4.2 dan android 5.1, ditemukan hasil diantaranya :

1. Malware ahmyth memerlukan proses booting terlebih dahulu pada perangkat android sehingga setelah booting malware ahmyth dapat menjalankan mainservice secara otomatis, ketika mainservice telah dijalankan maka malware ahmyth akan melakukan broadcast guna

menemukan alamat ip dan alamat mac dari C&C server yang akan melakukan remote command terhadap malware ahmyth tersebut, setelah alamat C&C ditemukan maka malware ahmyth akan mengirimkan informasi perangkat yang terinfeksi dan menunggu perintah selanjutnya dari C&C server, malware ahmyth ini dapat melakukan akses/download direktori dan file, melakukan pemotretan secara rahasia, melakukan perekaman audio secara rahasia, mengakses posisi perangkat pada peta secara realtime, mengakses pesan masuk, melakukan pengiriman sms secara remote, dan mengakses kontak list beserta daftar riwayat panggilan telepon.

2. Langkah pencegahan yang dapat dilakukan untuk mencegah dan menghindari terinfeksi dari malware ahmyth yaitu dengan tidak memasang aplikasi dari sumber yang tidak dipercaya, disable fitur install dari sumber tidak terpercaya yang terdapat pada developer option, pasang secreen lock, dan install aplikasi keamanan seperti anti-virus yang terpercaya agar perangkat terhidar dari malware ahmyth.

5. SARAN

Saran ini ditujukan untuk pengerjaan penelitian berikutnya, melalui laporan ini diharapkan: penelitian ini dilakukan penelitian menggunakan berbagai tool seperti winrar, apktool, jd gui, dex2jar, axmlprinter untuk melakukan analisis statis dan untuk melakukan analisis dinamis menggunakan inspeckage dan wireshark. Menganalisis menggunakan software diatas dibutuhkan waktu yang banyak karena beberapa analisis harus dilakukan secara manual, penelitian selanjutnya diharapkan dapat mengembangkan sistem yang dapat menganalisis secara otomatis menggunakan machine learning sehingga analisis terhadap sampel malware yang masif lebih cepat dan efisien.

DAFTAR PUSTAKA

[1.] Rubayyi Alghamdi “Android Platform Malware Analysis” (2015), (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 1, 2015.

[2.] Yesi Novaria Kunang “Analisis Forensik Malware Pada Platform Android”(2014). Konferensi Nasional Ilmu Komputer (KONIK) 2014 ISSN : 2338-2899

[3.] Triawan Adi Cahyanto “Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis” (2017). JUSTINDO, Jurnal Sistem & Teknologi Informasi Indonesia, Vol. 2, No. 1, Februari 2017

[4.] Shabtai, A., Kanonov, U., Elovici, Y. et al. J Intell Inf Syst (2012) 38: 161. https://doi.org/10.1007/s10844-010-0148-x. Deutsche Telekom Laboratories at Ben-Gurion University, Department of Information Systems Engineering, Ben-Gurion University, Be’er Sheva 84105, Israel

[5.] Muhammad Habibi “Implementation Of Malware Detection Service On Android” (2017) ISSN : 2442-5826 e-Proceeding of Applied Science : Vol.3, No.3 Desember 2017 | Page 1839

[6.] Fan Yuhui “ The Analysis of Android Malware Behaviors “ (2015), International Journal of Security and Its Applications Vol. 9, No. 3 (2015), pp. 335-346, http://dx.doi.org/10.14257/ijsia.2015.9.3.26

[7.] Vibha Manjunath, "Reverse engineering of Malware on Android" sans.org, Aug31, 2012. [Online]. available: https://sansorg.egnyte.com/dl/8zCSqZACzb

[8.] Van der Veen, Victor. (2013). Dynamic Analysis of Android Malware. 10.13140/2.1.2373.4080. VU University Amsterdam, Faculty of Sciences, Department of Computer Sciences, Internet & Web TechnologyM aster thesis ,

[9.] Kapratwar, Ankita, "Static and Dynamic Analysis for Android Malware Detection" (2016). Master's Projects. 488. DOI: https://doi.org/10.31979/etd.za5p-mqce, ttps://scholarworks.sjsu.edu/etd_projects/488

[10.] Adenansi, Retno, and Lia Ayu Novarina. "Malware dynamic." JOEICT (Jurnal of Education and Information Communication Technology) Volume1, Nomor1, Tahun2017:37–43, https://jurnal.stkippgritulungagung.ac.id/index.php/joeict/article/view/91/54