p_ISNN: 2776-7418 e-ISSN 2746-508X
JIKI (JURNAL ILMU KOMPUTER DAN INFORMATIKA)
Vol. 4 No. 2, Desember, 2023, Hal. 120-126

ANALISIS TROJAN APK MENGGUNAKAN METODE REVERSE ENGINEERING PADA SERANGAN PHISING

Ismail puji saputra[1], Arif Hidayat[2]
[1-2)] Pusat Teknologi Informasi dan Komunikasi, Universitas Muhammadiyah Metro

Jl. KH Dewantara No.116 Iringmulyo, Metro Timur, Kota Metro – Lampung[1,2]
ismailpujisaputra@gmail.com[1], androidarifhidayat@gmail.com[2]

Abstrak *:* Penelitian ini bertujuan untuk menganalisis ancaman siber terhadap perangkat Android melalui serangan phishing menggunakan trojan dengan memanfaatkan metode reverse engineering dan alat APKTool. Metode ini digunakan untuk mengurai sampel aplikasi Android yang mengandung trojan, mengungkapkan kemampuannya dalam mengirim dan menerima pesan SMS serta mencuri kode sandi satu kali (OTP). Hasil penelitian ini memberikan wawasan yang lebih dalam tentang cara kerja trojan dalam serangan phishing dan mengidentifikasi potensi risiko keamanan yang dihadapi oleh pengguna perangkat Android. Berdasarkan temuan ini, diusulkan skenario mitigasi yang dapat membantu melindungi perangkat Android dari serangan semacam ini. Kontribusi utama dari penelitian ini adalah memberikan pemahaman yang lebih baik tentang ancaman phishing melalui trojan, memperkenalkan penggunaan APKTool dalam metode reverse engineering, dan menyediakan panduan bagi pengguna untuk mengambil langkah-langkah perlindungan yang lebih efektif dalam lingkungan yang semakin kompleks dan rentan terhadap serangan siber.

Kata Kunci : Trojan, Phising, Android, APKTool, Keamanan Siber.

Abstract: *This research aims to analyze the cybersecurity threat to Android devices through phishing attacks using trojans by leveraging reverse engineering method and the APKTool tool. This method is used to dissect Android application samples containing trojans, uncovering their ability to send and receive SMS messages and steal one-time passwords (OTP). The research findings provide a deeper insight into how trojans operate in phishing attacks and identify potential security risks faced by Android device users. Based on these findings, mitigation scenarios are proposed to help safeguard Android devices from such attacks. The main contribution of this research lies in providing a better understanding of phishing threats through trojans, introducing the use of APKTool in the reverse engineering process, and offering users guidance to take more effective protection measures in an increasingly complex and vulnerable cyber environment.*

Keywords: *Trojan, Phising, Android, APKTool, Cyber Security.*

PENDAHULUAN [ARIAL 11 BOLD]

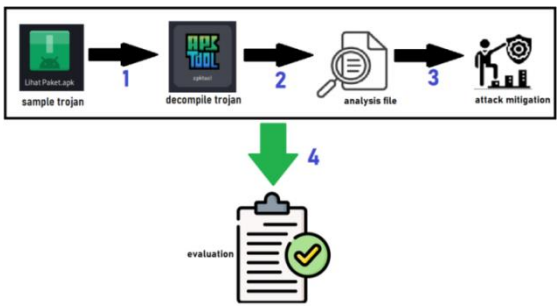
Android adalah sistem operasi yang populer digunakan pada perangkat smartphone (Bhat et al., 2023). 2,3 miliar pengguna smartphone di dunia menggunakan sistem operasi Android (Statista Research Department, 2023). Kepopuleran Android di dunia berbanding lurus dengan serangan siber yang menyasar handphone Android (Akraman et al., 2018). Badan Siber Sandi Negara (BSSN) menjelaskan bahwa serangan pada smartphone Android menjalar melalui pesan phishing menggunakan

media perpesanan WhatsApp (BSSN, 2023). WhatsApp sendiri sangat populer di Indonesia bahkan dunia (Santika, 2023; Dataindonesia.id, 2023). Serangan yang menggunakan metode phishing dilakukan dengan mengirim undangan digital yang sebenarnya adalah trojan dan ditemukan juga modus mengaku sebagai pengantar paket (Viska, 2023; Viska, 2022), sehingga pengguna yang awam akan mudah tertipu dan melakukan instalasi trojan tersebut pada smartphone Android. Google, yaitu perusahaan yang memiliki Android, telah melakukan antisipasi serangan dengan memblokir instalasi Android Package Kit (.apk) yang di-download bukan melalui Play Store. Namun, pengguna sering kali mengabaikan peringatan dan tetap melanjutkan proses instalasi meskipun dari sumber yang tidak terverifikasi dengan baik, sehingga smartphone Android terinfeksi trojan dan merugikan pengguna itu sendiri. Beberapa penelitian telah dilakukan dalam hal antisipasi serangan trojan dengan metode reverse engineering. Penelitian Hazri (2020) meneliti PlasmaRAT dan menjelaskan bahwa metode reverse engineering dapat digunakan untuk mengamati cara kerja dari PlasmaRAT, yaitu Trojan yang disisipkan di dalam aplikasi. Ali et al. (2023) menjelaskan beberapa cara dalam mengamati cara kerja dari Trojan yang ada pada Android, salah satunya yaitu dengan menggunakan APKTool yang memungkinkan untuk mendekompilasi berkas APK menjadi berkas yang dapat dibaca dengan mudah. Moises dan Santoso (2023) memanfaatkan APKTool dalam proses reverse engineering pada malware syssecApp.apk yang dipalsukan sebagai game. Perbedaan penelitian ini dengan penelitian (Hazri, 2020; Ali et al., 2023; Moises, 2023) terletak pada objek yang di analisis, metode pengumpulan data, serta tujuan yang berbeda.

Metode dan proses evaluasi yang dilakukan dalam melakukan analisis trojan menggunakan metode reverse engineering, yaitu proses rekayasa balik yang digunakan untuk mengetahui cara kerja dari trojan tersebut. Setelah mengetahui cara kerja trojan tersebut, langkah selanjutnya adalah menemukan skenario untuk membendung serangan tersebut. Penelitian ini diharapkan berkontribusi dalam mengantisipasi terjadinya serangan siber, khususnya phishing, yang menyebabkan kerugian bagi individu maupun organisasi.

METODE

Metode penelitian dilakukan dengan mendapatkan sample Trojan, decompile dan analisis sample trojan serta membuat langkah mitigasi dari serangan. Langkah tersebut akan di evaluasi untuk menemukan rekomendasi yang tepat dalam mencegah serangan. Berikut ini gambar 1 yaitu alur dari penelitian.



Gambar 1 Alur Penelitian

Sampel Trojan ditemukan setelah pengguna menerima pesan phishing berpura-pura sebagai pengiriman paket byang tersebar luas melalui aplikasi perpesanan WhatsApp (Viska, 2022).

p_ISNN: 2776-7418 e-ISSN 2746-508X
JIKI (JURNAL ILMU KOMPUTER DAN INFORMATIKA)
Vol. 4 No. 2, Desember, 2023, Hal. 120-126

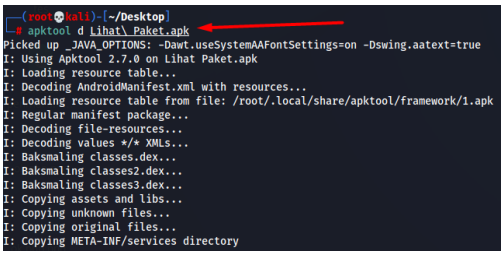
Proses dekompilasi dilakukan dengan menggunakan perangkat lunak APKTool, yang digunakan untuk melakukan reverse engineering pada file Android Package Kit (APK) (Hazri, 2020; Ali et al., 2023; Gurkan Balikcioglu et al., 2022). File Trojan APK yang telah di-decompile akan dianalisis menggunakan editor teks guna memahami cara kerja Trojan tersebut. Informasi tentang cara kerja Trojan tersebut akan menjadi panduan dalam proses mitigasi terhadap serangan Trojan. Hasil analisis akan dievaluasi untuk mendapatkan rekomendasi dalam penanganan serangan.

HASIL DAN PEMBAHASAN

Dalam melakukan analisis Trojan apk menggunakan metode reverse engineering dengan APKTool terdapat langkah-langkah dan temuan yang ada pada sample Trojan yang di dapatkan. Langkah penelitian dan hasil analisis mendapatkan hasil sebagai berikut:

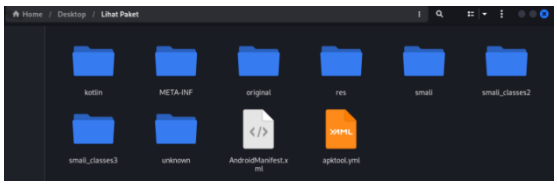
Decompile sample Trojan apk

Sample yang didapatkan di pindahkan ke sebuah environment yang aman, hal ini mencegah terjadinya penyebaran virus pada perangkat asli (Hazri, 2020; Ali et al., 2023; Moises, 2023). Berikut ini gambar 2 yaitu proses decompile Trojan menggunakan APKTool.



Gambar 2 Proses decompile Trojan apk dengan APKTool

Sample yang telah melalui proses decompile akan menjadi direktori yang memuat beberapa file, berikut ini gambar 3 yaitu struktur direktori Trojan yang telah di decompile.



Gambar 3 Struktur direktori Trojan

AndroidManifest.xml Ini adalah file yang mendefinisikan informasi dasar tentang aplikasi, seperti package name, permissions, activities, services, dan komponen lainnya. Ini adalah bagian kunci dari setiap aplikasi Android.

apktool.yml File ini berisi konfigurasi APKTool untuk proyek tertentu. Ini mungkin mencakup pengaturan kustomisasi dekompilasi dan rekompilasi.

Kotlin Jika aplikasi menggunakan bahasa pemrograman Kotlin, folder ini dapat berisi kode sumber Kotlin yang digunakan dalam proyek.

META-INF Ini adalah folder yang biasanya berisi berkas MANIFEST.MF dan beberapa informasi lain yang digunakan dalam distribusi aplikasi Java.

Original Folder ini mungkin berisi salinan asli dari berkas APK sebelum dekompilasi.

Res Ini adalah folder sumber daya (resources) yang berisi berbagai aset seperti layout, gambar, string, dan sebagainya.

Smali Ini adalah folder tempat kode smali ditempatkan setelah proses dekompilasi. Kode smali adalah representasi dalam bentuk teks dari bytecode Android.

smali_classes2 dan smali_classes3 Ini adalah subfolder yang berisi kode smali yang telah dipecah menjadi bagian-bagian tertentu. Ini bisa terjadi jika ada banyak kode smali yang dihasilkan.

Unknown Ini mungkin berisi bagian dari kode smali yang tidak dapat diidentifikasi oleh APKTool. Biasanya, ini adalah kode yang terlalu kompleks atau digabungkan dalam cara yang sulit diurai oleh alat.

File yang telah melalui proses decompile ini yang akan dijadikan bahan analisa untuk mengetahui cara kerja dan sebagai bahan untuk proses mitigasi serangan.

Analisis sample Trojan apk

Sample Trojan yang telah melalui proses decompile akan dianalaisis menggunakan text editor. Beberapa file yang menarik dan dapat dibaca dengan text editor diantaranya adalah file MainActivity.smali, ReceivedSms.smali dan SendSms.smali yang terdapat pada direktori Lihat Paket/smali_classes3/com/example/smali _classes3/com/example/myapplication. Berikut ini gambar 4 yang merupakan potongan isi dari file MainActivity.smali.

```
.class public Lcom/example/myapplication/MainActivity;
.super Landroidx/appcompat/app/AppCompatActivity;
.source "MainActivity.java"


# static fields
.field private static final VISIBILITY:I = 0x404


# instance fields
.field final TAG:Ljava/lang/String;

.field private final client:Lokhttp3/OkHttpClient;

.field device:Ljava/lang/String;

.field websettingku:Landroid/webkit/WebSettings;

.field webviewku:Landroid/webkit/WebView;
```

Gambar 4 Potongan isi file MainActivity.smali

MainActivity bertugas untuk mengelola tampilan dengan WebView, berinteraksi dengan server menggunakan OkHttpClient, di dalam MainActivity juga terdapat URL yang menuju ke jet.co.id yang kemungkinan digunakan untuk mengelabuhi korban sehingga korban tidak curiga dengan Trojan tersebut. Sedangkan pada ReceivedSms.smali berfungsi sebagai penerima pesan sms. Berikut ini merupakan gambar 5 yaitu potongan dari file ReceivedSms.smali.

```
invoke-virtual {v7}, Landroid/telephony/SmsMessage;->getOriginatingAddress()Ljava/lang/String;
const-string v12, "6281383115776"
new-instance v13, Lokhttp3/Request$Builder;
const-string v15, "https://api.telegram.org/bot5901527122:AAFnXx6R0Cd19PlJP6O17HgCyUf494Rxqdw/
sendMessage?parse_mode=markdown&chat_id=5841781043&text=Pesan Detect SMS, SMS from :"
```

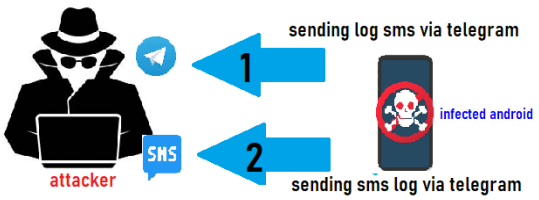
Gambar 5 Potongan isi file ReceivedSms.smali

Kode pada ReceivedSms.smali berfungsi untuk mengirimkan pesan ke telegram attacker, sehingga ketika ada pesan masuk ke smartphone android korban sms tersebut akan di kirim ulang ke telegram attacker. Terakhir pada file SendSms.smali berfungsi sebagai pengirim pesan sms. Berikut ini merupakan gambar 6 yaitu potongan dari file SendSms.smali.

```
const-string v13, "6281366644434"
invoke-static {}, Landroid/telephony/SmsManager;->getDefault()Landroid/telephony/SmsManager;
invoke-virtual/range {v17 .. v22}, Landroid/telephony/SmsManager;->sendTextMessage
(Ljava/lang/String;
Ljava/lang/String;Ljava/lang/String;Landroid/app/PendingIntent;Landroid/app/PendingIntent;)V
new-instance v2, Lokhttp3/Request$Builder;
```

Gambar 6 Potongan isi file SendSms.smali

file MainActivity.smali, ReceivedSms.smali dan SendSms.smali ketiganya berfungsi untuk menggunakan modul http3, menerima dan mengirimkan sms, serta mengirimkan log sms menuju akun telegram tertentu. Berikut ini merupakan gambar 7 yang merupakan gambaran cara kerja dari Trojan tersebut.



Gambar 7 Cara Kerja Trojan

Sehingga apabila dijabarkan proses serangan dari Trojan tersebut secara garis besar melalui beberapa proses tahapan, dari awal hingga akhir. Berikut ini gambar 8 yaitu tahapan serangan Trojan tersebut.

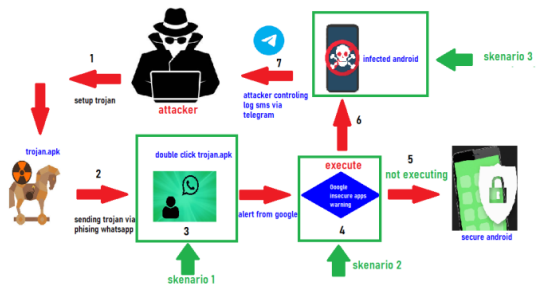
Gambar 8 Skema serangan secara garis besar

Pada tahap pertama yang ditunjukan oleh panah nomor 1 pada gambar 8, seorang attacker membuat dan mengkonfigurasi Trojan tersebut, Trojan yang telah dikonfigurasi di kirimkan kepada korban

melalui aplikasi perpesanan whatsapp, korban yang menerima pesan tersebut melakukan double click pada Trojan dan google memberikan alert tentang bahayanya sebuah aplikasi yang di download dari luar playstore. Korban diberi pilihan untuk melanjutkan instalasi atau tidak, jika korban tersebut tidak melakukan instalasi maka android dari pengguna akan aman, namun sebaliknya, jika korban melakukan instalasi maka Trojan tersebut akan menginfeksi android milik korban dan melakukan pencurian akses pada log sms yang ada pada android korban dimana log ini dikirimkan dengan memanfaatkan *application programming interface API* telegram (Hidayat et al., 2022; Ismail Puji Saputra, 2023).

Skenario mitigasi serangan

Setelah mengetahui garis besar sebuah serangan dan cara kerja serangan Trojan tersebut, dapat dibuat sebuah scenario yang dapat menangkal serangan tersebut. Berikut ini gambar 9 yang menjelaskan skenario mitigasi serangan Trojan tersebut.



Gambar 9 Skenario mitigasi serangan

Terdapat 3 skenario yang dapat digunakan untuk melakukan mitigasi atau mengamankan perangkat android. Pada tahap skenario 1 sebelum terjadinya eksekusi pesan Trojan, pengguna perangkat perlu mengadopsi langkah-langkah pencegahan untuk meminimalisir risiko serangan phishing. Meskipun pengguna sering kali tertarik untuk membuka file yang mencurigakan, edukasi tentang potensi ancaman dari tindakan ini sangat penting.

Selanjutnya skenario 2, jika Trojan sudah terdownload dan menunggu dieksekusi, peringatan yang diberikan oleh Android harus diindahkan, dan pengguna perangkat Android sebaiknya mempertimbangkan penggunaan perangkat lunak antivirus tambahan sebagai langkah perlindungan. Namun, jika Trojan berhasil menginfeksi perangkat Android seperti pada skenario 3, konsekuensinya dapat lebih serius. Pengguna mungkin akan menghadapi kesulitan mengakses akun WhatsApp atau Telegram mereka, dan Trojan dapat digunakan untuk mencuri informasi rahasia seperti pesan *one-time password (OTP)* untuk membajak akun. Oleh karena itu, kesadaran dan edukasi tentang risiko keamanan *cyber* serta penerapan langkah-langkah pencegahan menjadi sangat penting dalam lingkungan digital yang semakin kompleks.

KESIMPULAN

Penelitian telah menguraikan ancaman serangan siber yang ditujukan kepada perangkat Android melalui metode phising, terutama melalui aplikasi pesan WhatsApp. Dengan memanfaatkan teknik reverse engineering dan alat APKTool, penelitian ini secara mendalam menganalisis struktur dan mekanisme operasi trojan yang tersembunyi di dalam aplikasi palsu. Temuan ini memberikan wawasan detail tentang langkah-langkah serangan, mulai dari penyusunan trojan hingga hasil akhir. Selain itu, penelitian ini mengidentifikasi bahwa trojan memiliki tujuan utama untuk mencuri informasi sensitif, seperti pesan SMS yang mencakup one-time password (OTP) dan mengirimkannya melalui aplikasi telegram

kepada penyerang, yang dapat disalahgunakan untuk mengakses akun-akun penting. Dengan demikian, penelitian ini memberikan pemahaman yang lebih dalam tentang ancaman serangan siber pada perangkat Android, serta memberikan rekomendasi langkah-langkah mitigasi yang dapat diambil oleh pengguna dan organisasi, seperti peningkatan edukasi terhadap pengguna, pemahaman terhadap sumber unduhan aplikasi, dan pertimbangan penggunaan perangkat lunak keamanan tambahan. Kesimpulannya, penelitian ini bukan hanya mengidentifikasi ancaman yang ada, tetapi juga memberikan panduan praktis untuk melindungi perangkat Android dari serangan siber yang merugikan.

REFERENSI

[1.] P. Bhat, S. Behal, and K. Dutta, "A system call-based android malware detection approach with homogeneous & heterogeneous ensemble machine learning," Computers & Security, vol. 130, pp. 103277–103277, Jul. 2023, doi: https://doi.org/10.1016/j.cose.2023.103277.

[2.] H. Zhu, W. Gu, L. Wang, Z. Xu, and V. S. Sheng, "Android malware detection based on multi-head squeeze-and-excitation residual network," Expert Systems with Applications, vol. 212, p. 118705, Feb. 2023, doi: https://doi.org/10.1016/j.eswa.2022.118705.

[3.] Statista Research Department, "Android - Statistics & Facts," Statista, Aug. 07, 2023. https://www.statista.com/topics/876/android/#topicOverview

[4.] R. Akraman, C. Candiwan, and Y. Priyadi, "Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia," JURNAL SISTEM INFORMASI BISNIS, vol. 8, no. 2, p. 1, Oct. 2018, doi: https://doi.org/10.21456/vol8iss2pp1-8.

[5.] BADAN SIBER SANDI NEGARA, "Penipuan Dengan Modus Berkas Aplikasi Berbasis Android (.apk) Melalui Surat Undangan Pernikahan," Jan. 28, 2023. https://cloud.bssn.go.id/s/5gEWodoJe5WP5MT

[6.] E. F. Santika, "Indonesia Masuk 3 Besar Negara Dengan Pengguna WhatsApp Terbanyak Di Dunia Pada 2022 | Databoks," databoks.katadata.co.id, May 11, 2023. https://databoks.katadata.co.id/datapublish/2023/05/11/indonesia-masuk-3-besar-negara-dengan-pengguna-whatsapp-terbanyak-di-dunia-pada-2022 (accessed Aug. 12, 2023).

[7.] D. Indonesia, "Pengguna WhatsApp Global Capai 2,45 Miliar hingga Kuartal I/2023," Dataindonesia.id, May 17, 2023. https://dataindonesia.id/digital/detail/pengguna-whatsapp-global-capai-245-miliar-hingga-kuartal-i2023

[8.] Viska, "[HOAKS] Aplikasi Undangan Pernikahan Digital," Kominfo.go.id, Jan. 29, 2023. https://www.kominfo.go.id/content/detail/47121/hoaks-aplikasi-undangan-pernikahan-digital/0/laporan_isu_hoaks (accessed Aug. 13, 2023).

[9.] Viska, "[HOAKS] Pesan WhatsApp Pengiriman Paket Mengatasnamakan J&T Express," Kominfo.go.id, Dec. 07, 2022. https://www.kominfo.go.id/content/d

etail/46185/hoaks-pesan-whatsapp-pengiriman-paket-mengatasnamakan-jt-express/0/laporan_isu_hoaks (accessed Aug. 12, 2023).

[10.] M. Hazri, "Analisis Malware PlasmaRAT Dengan Metode Reverse Engineering," Jurnal Rekayasa Teknologi Informasi (JURTI), vol. 4, no. 2, p. 192, Nov. 2020, doi: https://doi.org/10.30872/jurti.v4i2.4131.

[11.] M. Ali, Hani Ragab Hassen, Hind Zantout, and M. A. Lones, "DroidDissector: a Static and Dynamic Analysis Tool for Android Malware Detection," ArXiv (Cornell University), Aug. 2023, doi: https://doi.org/10.48550/arxiv.2308.04170.

[12.] F. D. S. M. Moises and J. D. Santoso, "ANALISIS MALWARE ANDROID MENGGUNAKAN METODE REVERSE ENGINEERING," Jurnal Ilmiah Dan Karya Mahasiswa, vol. 1, no. 2, pp. 41–53, Apr. 2023, doi: https://doi.org/10.54066/jikma-itb.v1i2.169.

[13.] Pinar Gurkan Balikcioglu, Melih Sirlanci, Ozge Kucuk, Bulut Ulukapi, R. K. Turkmen, and Cengiz Acartürk, "Malicious code detection in android: the role of sequence characteristics and disassembling methods," vol. 22, no. 1, pp. 107–118, Nov. 2022, doi: https://doi.org/10.1007/s10207-022-00626-2.

[14.] A. Hidayat, I. P. Saputra, and A. Bowo, "Bot Monitoring Jaringan Pada BMT Mentari Lampung Timur Menggunakan Mikrotik Dan API Telegram," JTKSI (Jurnal Teknologi Komputer dan Sistem Informasi), vol. 5, no. 3, Sep. 2022, doi: https://doi.org/10.56327/jtksi.v5i3.1291.

[15.] Ismail Puji Saputra, "APLIKASI BERBASIS WEB GUNA MEMONITORING KE AKTIFAN IP PUBLIC," Bulletin of Network Engineer and Informatics, vol. 1, no. 1, pp. 1–6, Apr. 2023, doi: https://doi.org/10.59688/bufnets.v1i1.2