Syntax:
Journal of Software Engineering, Computer Science and Information Technology
p-ISSN: 2776-7027, e-ISSN: 2723-0538
Volume: 5, Nomer: 2, Desember 2024

Penerapan Tools JADX Pada Serangan Malware berbasis Android Menggunakan Metode NIST : Studi kasus Undangan.apk

Bashor Fauzan Muthohirin[1], Alfin Zahrotun Nasuhah[2]

Denar Regata Akbi[3]

[1,2,3] *Fakultas Teknik, Informatika, Universitas Muhammadiyah Malang, Malang, Indonesia*
Jl. Raya Tlogomas No. 246, Malang, 65144, Indonesia

[1]*bashorfauzan@umm.ac.id*, [2]*dnarregata@umm.ac.id*, [3]*alfinzahrotun@webmail.umm.ac.id*
Email Penulis Korespondensi: bashorfauzan@umm.ac.id

ABSTRAK

Perkembangan teknologi smartphone dengan sistem operasi Android yang pesat telah membuat pengguna menghabiskan rata-rata 5,3 jam per hari. Hal tersebut menjadikan smartphone dengan sistem operasi Android rentan terhadap ancaman malware, termasuk serangan melalui aplikasi berbahaya seperti Undang.apk yang didistribusikan melalui pesan WhatsApp. Serangan ini menggunakan teknik sosial *engineering* untuk melakukan menipuan, mencuri data pribadi, dan menyebabkan kerugian material kepada korban. Penelitian ini bertujuan untuk menganalisis malware Undang.apk menggunakan metode forensik NIST, Proses awal investigasi dilakukan dengan melakukan akuisisi barang bukti digital menggunakan MOBILedit Forensic Tool, identifikasi malware melalui VirusTotal, serta analisis struktur kode APK menggunakan JADX GUI. Hasil penelitian menunjukkan bahwa malware tersebut memanfaatkan izin berbahaya untuk membaca dan mengirim pesan korban ke bot Telegram milik pelaku. Laporan akhir menyajikan temuan penting yang tidak hanya dapat digunakan sebagai bukti dalam proses hukum, tetapi juga sebagai panduan mitigasi untuk mencegah ancaman serupa di masa mendatang.

Kata Kunci: Malware, Android, JADX, Forensics, NIST.

ABSTRACT

The rapid development of smartphone technology with the Android operating system has made users spend an average of 5.3 hours per day. This makes smartphones with the Android operating system vulnerable to malware threats, including attacks through malicious applications such as Undang.apk which are distributed via WhatsApp messages. This attack uses social engineering techniques to commit fraud, steal personal data, and cause material losses to victims. This study aims to analyze the Undang.apk malware using the NIST forensic method. The initial investigation process was carried out by acquiring digital evidence using the MOBILedit Forensic Tool, identifying malware through VirusTotal, and analyzing the APK code structure using JADX GUI. The results of the study showed that the malware utilized dangerous permissions to read and send victim messages to the perpetrator's Telegram bot. The final report presents important findings that can not only be used as evidence in legal proceedings, but also as a mitigation guide to prevent similar threats in the future.

Keywords: Malware, Android, JADX, Forensics, NIST.

Syntax:
Journal of Software Engineering, Computer Science and Information Technology
p-ISSN: 2776-7027, e-ISSN: 2723-0538
Volume: 5, Nomer: 2, Desember 2024

I. PENDAHULUAN

Perkembangan teknologi yang terus berkembang, maka akan mempermudah kita dalam mengakses informasi kapan pun dan dimana pun. Salah satu teknologi yang saat ini digunakan untuk mengakses informasi tersebut adalah *smartphone*. *Smartphone* adalah teknologi yang dapat digunakan dan dibawa oleh setiap orang dalam kegiatannnya sehari-hari. Menurut hasil laporan firma riset data.ai bertajuk "State of Mobile 2023" menunjukan 5,3 jam perhari pengguna internet di indonesia, hal tersebut menjadi yang tertinggi dibandingkan di seluruh dunia [1].

Intensitas yang cukup lama dalam penggunaan *smartphone* maka akan meningkatkan serangan pada pengguna *smartphone* tersebut. Terdapat berbagai cara dalam penyerangan yang dilakukan, seperti mengirimkan malware dengan jenis rasomeware tertentu. Berdasarkan data yang dirilis oleh Badan Siber dan Sandi Negara (BSSN) pada tahun 2023 ada 5 jenis malware jenis Luna Moth, WannaCry, Locky, LockBit, dan GandCrab [2].

Kerugian atas serangan malware tersebut menyebabkan kerugian pada korban mencapai US$ 9,2 T secara global [3]. Penelitian yang terdapat beberapa cara dalam melakukan serangan dicyberspace dengan metode Wade and Seek yang merupakan penerapan teori negosiasi sandera tradisional yang digunakan untuk membantu bisnis mengurangi biaya serangan *ransomware*[4].

Penelitian yang dilakukan oleh [5] pada penelitian ini menggunakan metode Maat untuk menggantikan strategi pelabelan berbasis ambang batas yang tidak konsisten di VirusTotal. Maat menggunakan pembelajaran mesin (ML) untuk memberi label aplikasi Android secara akurat dan konsisten, berdasarkan hasil pemindaian dari 60 pemindai antivirus. Evaluasi terhadap 53.000 aplikasi Android selama satu tahun menunjukkan bahwa metode ML ini lebih efektif dalam memberikan pelabelan yang akurat dan meningkatkan deteksi malware, dibandingkan dengan strategi berbasis ambang batas.

Penelitian yang dilakukan oleh [6], pada penelitian ini membandingkan empat *tools* forensik MOBILedit, Oxygen Forensic, Autopsy, dan Andriller yang digunakan untuk mengekstraksi bukti dari perangkat Android dengan versi yang berbeda. Penelitian ini mengevaluasi efektivitas alat-alat tersebut dengan menganalisis data yang diekstraksi, mengidentifikasi data penting dan data yang tidak terbaca, serta menilai potensi bukti tersebut diterima di pengadilan. Hasil penelitian menunjukkan bahwa meskipun alat sumber terbuka dapat mengekstrak data yang cukup banyak.

Penelitian yang dilakukan oleh [7], dalam penelitian tersebut, JADX digunakan sebagai salah satu alat *reverse engineering* yang sangat efektif untuk membongkar atau menganalisis file APK Android. Alat ini digunakan untuk *reverse engineering* pada aplikasi Android menjadi *source code* sehingga memungkinkan penyerang untuk memahami struktur dan logika aplikasi. Setelah *source code* diperoleh, aplikasi dapat dengan mudah dimodifikasi atau disisipkan dengan kode berbahaya, dan kemudian disusuan ulang menjadi aplikasi yang disebut *repackaged app*.

Penelitian yang dilakukan oleh [8] memanfaatkan teknik pembelajaran mesin untuk deteksi malware pada file APK, dengan fokus pada efisiensi waktu dan sumber daya dibandingkan pendekatan non-pembelajaran mesin. Penelitian ini mencakup tiga fase utama: Pengumpulan File Android, Dekompilasi, dan Penambangan Fitur, dengan 15.508 file malware dan 4.000 file benign yang telah dikumpulkan. Proses dekompilasi dilakukan menggunakan dekompiler online JADX, yang menghasilkan struktur file APK yang telah direkayasa ulang, memungkinkan pengelolaan dan pemrosesan data besar untuk deteksi malware..

Penelitian yang dilakukan oleh [9] berjudul "*Forensic analysis on discord application using the National Institute of Standards and Technology (NIST) Method*" mengeksplorasi pengambilan pesan yang dihapus dari percakapan desktop Discord menggunakan kerangka kerja NIST SP 800-86. Penelitian ini menggunakan alat seperti FTK Imager, ChromeCacheView, dan Autopsy untuk mengekstraksi artefak digital. FTK Imager mencapai akurasi 16,67%, dengan artefak berupa file gambar, sedangkan ChromeCacheView lebih efektif dengan tingkat akurasi 73,33%, berhasil mengambil berbagai artefak seperti file gambar, video, pesan teks, akun, dan email, meskipun tidak semua pesan teks dapat diambil. Autopsy, dengan akurasi 33,33%, mampu mengambil gambar dan email. Temuan ini menunjukkan perbedaan efektivitas alat dalam investigasi forensik di Discord, sekaligus menyoroti pentingnya metode yang komprehensif untuk menangani penyalahgunaan dan pelanggaran di platform tersebut[10].

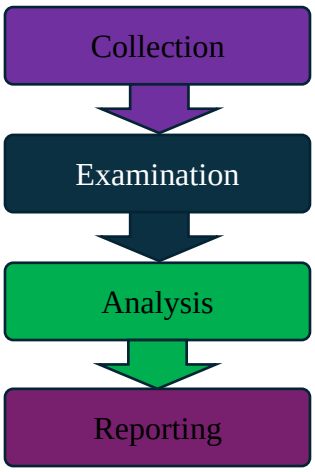
Berdasarkan fenomena tersebut, penelitian ini bertujuan Penerapan Tools JADX Pada Serangan Undang.apk berbasis Android Menggunakan Metode NIST (National Institute of Standards and Technology). Penelitian ini diharapkan dapat memberikan kontribusi

Syntax:
Journal of Software Engineering, Computer Science and Information Technology
p-ISSN: 2776-7027, e-ISSN: 2723-0538
Volume: 5, Nomer: 2, Desember 2024

dalam memahami serangan malware dan strategi mitigasinya, khususnya pada sistem operasi berbasis Android.

II. METODELOGI PENELITIAN

Pada penelitian ini kami menggunakan metode NIST[11] (National Institute of Standards and Technology), alur NIST dapat dilihat pada gambar 1 dibawah ini.



Gambar 1. Alur Penelitian

Collection, Tahap awal dimulai dengan pengumpulan barang bukti, di mana pelaku mengirimkan file APK berbahaya kepada korban melalui pesan singkat WhatsApp Selanjutnya, dilakukan akuisisi data digital menggunakan MOBILedit Forensic Tool. Proses ini mencakup dokumentasi barang bukti digital dan melakukan imaging smartphone untuk menciptakan cadangan (*backup*) guna menjaga integritas data selama analisis.

Examination, Setelah seluruh aplikasi yang terinstal pada perangkat korban dianalisis menggunakan VirusTotal, memberikan informasi jika undangan.apk terdeteksi terdapat malware yang ada didalamnya. Pada gambar 6 menejlaskan jika terdapat 4 ijin yang seharusnya tidak diberikan. Kemudian Pada tahap ini, dilanjutkan untuk melakukan pengujian menggunakan JADX GUI untuk menelusuri bukti digital lebih dalam, termasuk mencari informasi penting seperti alamat akun Telegram yang digunakan pelaku.

Analysis, dilakukan berdasarkan hasil pengumpulan data dan pengujian dengan JADX GUI terhadap file APK yang teridentifikasi sebagai ransomware. Tahapan analisis meliputi:

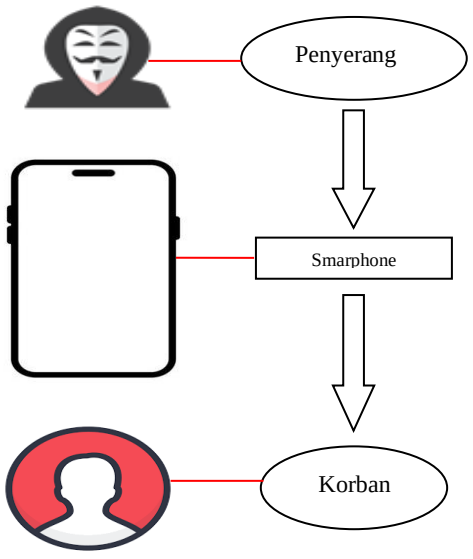
- Analisis Statis: Memeriksa struktur kode dalam APK menggunakan JADX GUI untuk memahami mekanisme kerja malware. Ditemukan bahwa malware memanfaatkan izin berbahaya seperti RECEIVE_SMS, READ_SMS, dan SEND_SMS untuk membaca dan mengirim pesan dari perangkat korban.
- Penelusuran Aktivitas: Malware ini diketahui mengirim data ke bot Telegram milik pelaku menggunakan API Telegram, mengonfirmasi modus operandi serangan.

Reporting, Tahap terakhir adalah penyusunan laporan berdasarkan temuan investigasi. Laporan ini meliputi:

- Penjelasan rinci tentang cara kerja malware dalam mengakses dan mengeksploitasi data pribadi korban.
- Bukti yang ditemukan, termasuk alamat API Telegram yang digunakan pelaku, dapat menjadi bahan pertimbangan dalam proses hukum.
- Laporan ini memberikan gambaran menyeluruh tentang bagaimana serangan terjadi dan langkah-langkah yang diperlukan untuk pencegahan di masa depan.

III. HASIL DAN PEMBAHASAN

Hasil dari penelitian ini dilakukan dengan melakukan akuisisi terhadap malware yang dikirim melalui pesan singkat WhatsApp yang dikirim oleh pelaku kepada korban. Kemudian, malware ini dilakukan akusisi dan di lakukan analisis forensik. Berikut ini adalah proses akuisisi menggunakan metode NIST:



Gambar 2. Tahap Collection

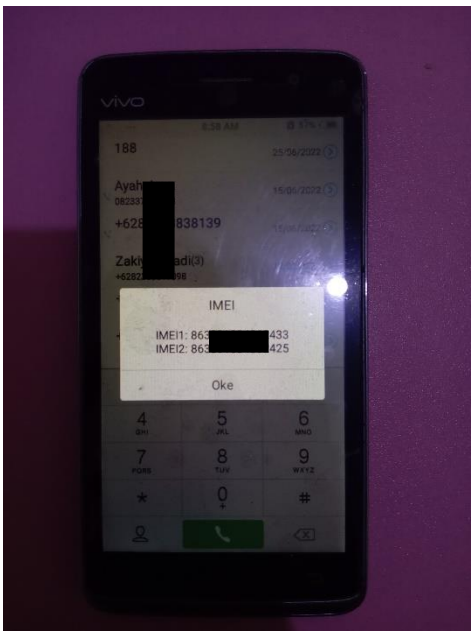
Syntax:
Journal of Software Engineering, Computer Science and Information Technology
p-ISSN: 2776-7027, e-ISSN: 2723-0538
Volume: 5, Nomer: 2, Desember 2024

Gambar 2 menunjukkan skenario proses penelitian untuk memperoleh barang bukti. Dalam skenario ini, penyerang mengirimkan malware undang.apk ke smartphone korban melalui pesan instan WhatsApp. Korban kemudian membuka pesan tersebut dan mengunduh file yang dilampirkan. Setelah file diunduh, malware secara otomatis terinstal pada perangkat korban tanpa sepengetahuannya.

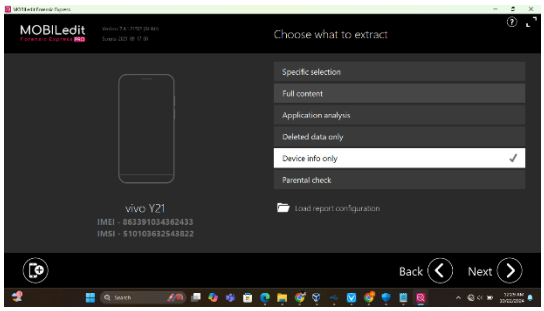
A. *Collection*

Proses investigasi dimulai dengan pengumpulan barang bukti dari perangkat yang memiliki spesifikasi merek Vivo Y21 dengan sistem operasi Android Lollipop 5.1. Proses akuisisi data dilakukan menggunakan alat forensik digital, yaitu MOBILedit Forensic. Pada tahap collection, barang bukti diperoleh dari skenario serangan di mana penyerang mengirimkan malware melalui pesan instan WhatsApp kepada korban. Peneliti kemudian mengumpulkan bukti digital tersebut dan melanjutkan dengan proses validasi sebelum data dianalisis lebih lanjut.

Proses validasi dilakukan untuk mencocokkan nomor IMEI perangkat Android dengan nomor IMEI yang terdeteksi oleh alat MOBILedit Forensic. Hasil validasi dapat dilihat pada Gambar 3.



Gambar 3. Nomor IMEI dari *smartphone* korban

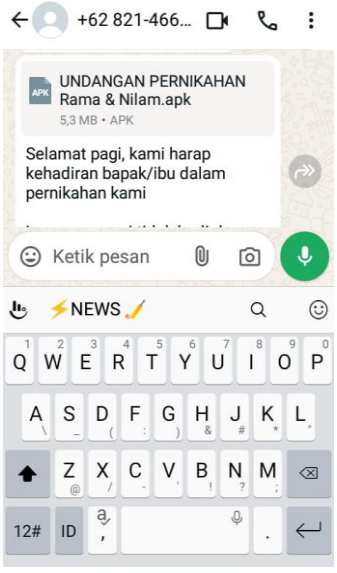


Gambar 4. Nomor IMEI dari MOBILedit Forensic.

Gambar 3 merupakan nomor email IMEI1 : 86339********433 dan IMEI2 : 86339********425. Pada gambar 4 ditemukan 86339********433. Maka dapat dismpulkan bahwa Nomor IMEInya sama dan dapat dilakukan pada tahap selanjutnya. tools ini digunakan untuk menjaga keaslian barang bukti digital agar tidak rusak atau hilang selama proses investigasi dan analisis.

B. *Examination*

Pelaku kejahatan melancarkan serangan social engineering yang dimulai dengan mengirimkan pesan WhatsApp kepada korban. Seperti gambar berikut ini.



Gambar 6. Bukti pengiriman malware

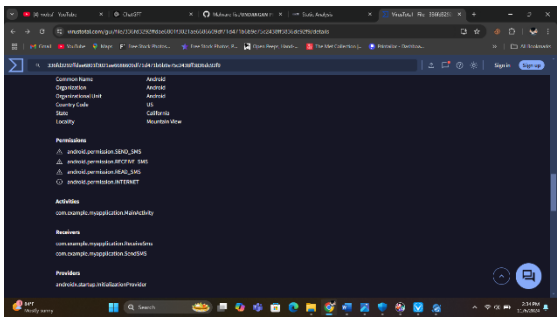
Gambar 6. merupakan pesan yang berisi undangan.apk pernikahan digital yang dikemas secara meyakinkan dengan caption yang diberikan. namun secara mencurigakan dikirim dalam format file APK. Pada saat instalasi, aplikasi berbahaya ini meminta berbagai izin akses yaitu pengiriman SMS yang didapatkan di ponsel korban kepada

Syntax:
Journal of Software Engineering, Computer Science and Information Technology
p-ISSN: 2776-7027, e-ISSN: 2723-0538
Volume: 5, Nomer: 2, Desember 2024

sebuah BOT telegram. Korban yang tidak waspada memberikan semua izin yang diminta, sehingga malware berhasil terinstal secara sempurna di perangkat Android korban. Hal ini berakibat, korban mendapati pengurangan saldo dari akun rekening yang terdaftar di perangkat tersebut, mengindikasikan bahwa kredensial perbankan telah berhasil dieksploitasi oleh pelaku.

C. *Analysis*

Supaya memudahkan dalam melakukan analisa, dilakukan proses filtering pada artefak apapun yang terhubung maupun diterima selama satu bulan terakhir dari hari dimana kasus terjadi, seperti panggilan, SMS, Wi-Fi yang terhubung, aplikasi yang diinstall, dan lain-lain. Selanjutnya, dilakukan pemeriksaan terhadap seluruh aplikasi yang terpasang sebagai deteksi dini kemungkinan adanya malware pada perangkat menggunakan alat forensik VirusTotal. Seperti terlihat pada gambar 5

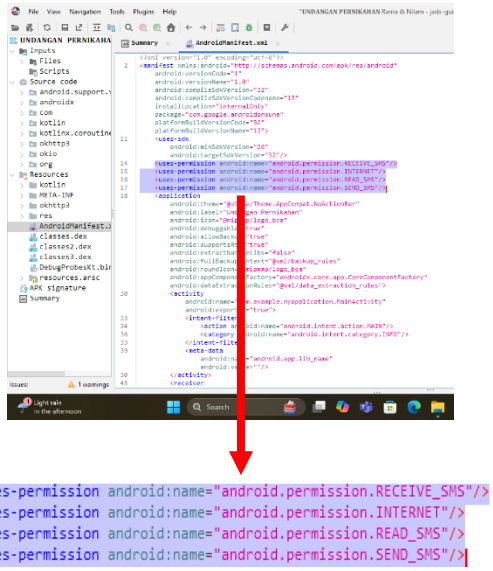


Gambar 5. Hasil deteksi undangan.apk

Gambar 5 menunjukkan hasil deteksi awal terhadap aplikasi undangan.apk menggunakan alat forensik VirusTotal. Pada pemeriksaan ini, ditemukan sejumlah permissions yang berpotensi berbahaya, yaitu: RECEIVE_SMS, READ_SMS, SEND_SMS dan INTERNET.

Berdasarkan hasil tersebut, dilakukan analisis lebih mendalam untuk memverifikasi dan memahami peran permissions tersebut dalam aktivitas aplikasi. Untuk analisis ini, peneliti menggunakan alat Jadx GUI guna mengakses dan membaca struktur internal aplikasi, termasuk file AndroidManifest.xml.

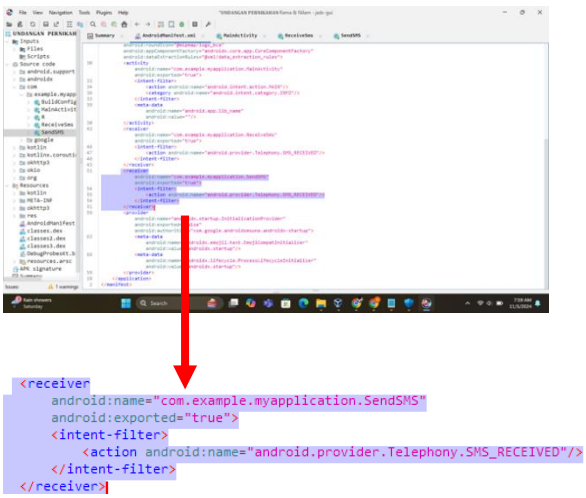
Pada file AndroidManifest.xml, ditemukan permissions yang sesuai dengan laporan VirusTotal, seperti gambar 6.



```
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.SEND_SMS"/>
```

Gambar 6. Permision yang ditemukan

Gambar 6 ditemukan permision yang berbahaya seperti *RECEIVE_SMS*, *INTERNET*, *READ_SMS*, *SEND_SMS*. yang menegaskan bahwa aplikasi undangan.apk memiliki kemampuan untuk membaca, menerima, dan mengirim pesan SMS tanpa sepengetahuan pengguna. Permissions ini memberikan indikasi kuat bahwa aplikasi tersebut dirancang untuk aktivitas mencurigakan yang perlu dianalisis lebih lanjut.



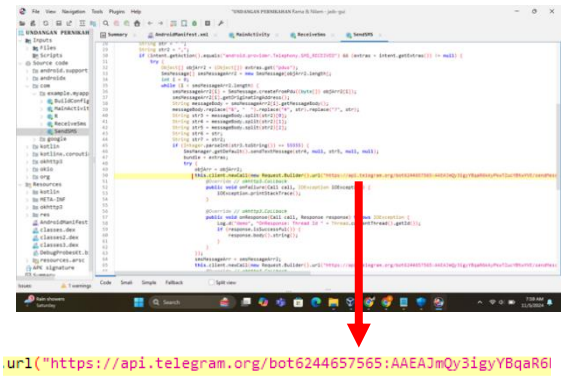
```
<receiver
    android:name="com.example.myapplication.SendSMS"
    android:exported="true">
    <intent-filter>
        <action android:name="android.provider.Telephony.SMS_RECEIVED"/>
    </intent-filter>
</receiver>
```

Gambar 7. Fungsi untuk menerima sms

Gambar 7 menampilkan fungsi dalam aplikasi undangan.apk yang bertanggung jawab untuk menerima SMS dari perangkat korban. Fungsi ini memanfaatkan permission RECEIVE_SMS dan READ_SMS, yang memungkinkan aplikasi

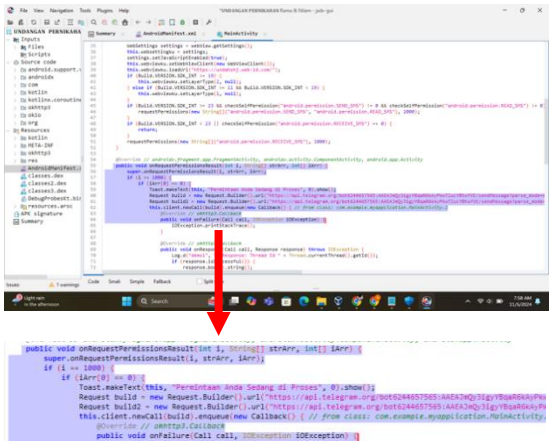
Syntax:
Journal of Software Engineering, Computer Science and Information Technology
p-ISSN: 2776-7027, e-ISSN: 2723-0538
Volume: 5, Nomer: 2, Desember 2024

membaca pesan SMS tanpa persetujuan eksplisit dari pengguna.



Gambar 8. Fungsi mengirim sms

Gambar 8 menunjukkan fungsi lain yang digunakan untuk mengirimkan SMS secara otomatis. Fungsi ini menggunakan permission SEND_SMS untuk mengirim pesan dari perangkat korban ke pihak ketiga, tanpa sepengetahuan pemilik perangkat.



Gambar 9. Method onRequestPermissionsResult

Pada Gambar 9, ditunjukkan kode dari method *onRequestPermissionsResult*, yang berperan dalam menangani hasil permintaan izin dari pengguna. Jika izin yang diminta oleh aplikasi disetujui, method ini secara otomatis akan mengirimkan data pesan ke sebuah bot Telegram.

Analisis lebih lanjut dilakukan pada file ReceiveSMS dan SendSMS. Dari analisis ini, ditemukan bahwa aplikasi memanfaatkan API Telegram dengan alamat: **https://api.telegram.org/bot6244657565.**

API ini digunakan untuk mentransfer data pesan SMS dari perangkat korban ke pelaku melalui bot Telegram. Fakta ini menunjukkan bahwa aplikasi undangan.apk dirancang untuk mencuri data SMS korban dan menyampaikannya secara real-time ke pelaku melalui platform Telegram.

D. *Reporting*

Setelah dilakukan analisis kode menggunakan Jadx GUI, disusun laporan yang merangkum hasil analisis kode pada APK malware bernama Undangan Digital. Laporan ini mencakup detail mengenai kode-kode berbahaya yang terdapat di dalam APK tersebut, serta metode kerja malware dalam mencuri data korban. Berdasarkan analisis yang dilakukan, diketahui bahwa malware ini menggunakan bot Telegram sebagai media untuk mengirimkan data privasi korban, khususnya SMS.

IV. KESIMPULAN

Penelitian ini berhasil mengidentifikasi dan menganalisis serangan malware pada file undangan.apk berbasis Android dengan menggunakan Tools JADX dan Metode NIST untuk penyelidikan forensik digital. Proses investigasi dimulai dengan pengumpulan barang bukti dari perangkat Android yang terinfeksi dan akuisisi data menggunakan MOBILedit Forensic Tool untuk memastikan integritas bukti. Pemeriksaan APK yang diunduh korban melalui pesan WhatsApp menunjukkan bahwa file tersebut mengandung elemen berbahaya, seperti permission RECEIVE_SMS, READ_SMS, dan SEND_SMS yang memungkinkan malware mengakses dan mengirim SMS tanpa izin. Analisis kode juga mengungkapkan bahwa aplikasi ini menggunakan API Telegram untuk mengirimkan data SMS ke server pelaku. Penelitian ini menegaskan pentingnya kesadaran pengguna dalam mengunduh aplikasi dari sumber yang tidak relevan dan penggunaan alat forensik seperti JADX serta pemeriksaan awal dengan VirusTotal untuk mendeteksi aplikasi berbahaya. Rekomendasi utama adalah penggunaan perangkat lunak keamanan yang kuat, pemantauan izin aplikasi secara rutin, dan edukasi bagi pengguna untuk mencegah serangan serupa di masa depan. Metode NIST terbukti efektif dalam mendeteksi, menganalisis, dan memberikan solusi terhadap ancaman keamanan malware berbasis Android.

REFERENSI

[1] "Indonesia Jadi Negara Paling Kecanduan HP di 2023 - GoodStats Data." Accessed: Dec. 06, 2024. [Online]. Available: https://data.goodstats.id/statistic/indonesia-jadi-negara-paling-kecanduan-hp-di-2023-BH8MU

[2] "5 Ransomware Paling Banyak Ditemukan di Indonesia | Databoks." Accessed: Oct. 26, 2024. [Online]. Available: https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/8356afa334da6d9/5-ransomware-paling-banyak-ditemukan-di-indonesia

[3] A. Mutia, "Kerugian Akibat Kebocoran Data Financial (2021)," *databoks.katadata.co.id*, 2022. [Online]. Available: https://databoks.katadata.co.id/layanan-konsumen-kesehatan/statistik/83e746437b06b9c/ini-sederet-kerugian-yang-dialami-publik-akibat-kebocoran-data-finansial

[4] M. Wade, "Digital hostages: Leveraging ransomware attacks in cyberspace," *Business Horizons*, vol. 64, no. 6, pp. 787–797, Nov. 2021, doi: 10.1016/j.bushor.2021.07.014.

[5] A. Salem, S. Banescu, and A. Pretschner, "Maat: Automatically Analyzing VirusTotal for Accurate Labeling and Effective Malware Detection," *ACM Trans. Priv. Secur.*, vol. 24, no. 4, pp. 1–35, Nov. 2021, doi: 10.1145/3465361.

[6] R. M. Abou-Elzahab, M. F. Al Rahmawy, and T. T. Hamza, "Comparative Study of Different Mobile Forensic Tools for Extracting Evidence from Android Devices," *Mansoura Journal for Computer and Information Sciences*, vol. 16, no. 1, pp. 1–12, Jun. 2020, doi: 10.21608/mjcis.2020.321070.

[7] M. R. Khan, "Network Traffic Based Detection of Repackaged Android Apps via Mobile Fog Computing," *International Journal of Future Generation Communication and Networking*, vol. 14, no. 1, 2021.

[8] P. Agrawal and B. Trivedi, "Unstructured Data Collection from APK files for Malware Detection," *IJCA*, vol. 176, no. 28, pp. 42–45, Jun. 2020, doi: 10.5120/ijca2020920308.

[9] M. Koprawi and F. D. Ikram, "Forensic analysis on discord application using the National Institute of Standards and Technology (NIST) Method," *Jurnal Mandiri IT*, vol. 12, no. 1, Art. no. 1, Aug. 2023, doi: 10.35335/mandiri.v12i1.224.

[10] A. M. Afdal, Y. Salim, and A. R. Manga, "ANALISIS BUKTI DIGITAL FORENSIK PADA DISCORD MENGGUNAKAN METODE NATIONAL INSTITUTE OF STANDARDS TECHNOLOGY," *BUSITI*, vol. 3, no. 4, pp. 293–300, Nov. 2022, doi: 10.33096/busiti.v3i4.1425.

[11] R. Umar, I. Riadi, and B. F. Muthohirin, "Acquisition of Email Service Based Android Using NIST," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, pp. 263–270, Jul. 2018, doi: 10.22219/kinetik.v3i3.637.