DETEKSI *MALWARE* ANDROID DENGAN METODE *REVERSE ENGINEERING*

SKRIPSI

Oleh:

INDRA WICAKSONO
09011382025128

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN

DETEKSI *MALWARE* ANDROID DENGAN METODE *REVERSE ENGINEERING*

SKRIPSI

Program Studi Sistem Komputer

Jenjang S1

Oleh:

INDRA WICAKSONO

09011382025128

Palembang, 19 Juli 2024

Pembimbing I	Pembimbing II
Prof. Deris Stiawan, M.T., Ph.D.	**Nurul Afifah, M.Kom.**
NIP. 197806172006041002	**NIP. 199211102023212049**

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

AUTHENTICATION PAGE

ANDROID MALWARE DETECTION WITH REVERSE ENGINEERING METHOD

THESIS

Dept. of Computer System

Bachelor's Degree

By:

INDRA WICAKSONO

09011382025128

Palembang, 15 July 2024

Supervisor	Co-Supervisor
Prof. Deris Stiawan, M.T., Ph.D.	Nurul Afifah, M.Kom.
NIP. 197806172006041002	NIP. 199211102023212049

Acknowledge,

Head Of Computer Systems Departement

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

LEMBAR PERSETUJUAN

Telah di uji dan lulus pada:

Hari : Rabu

Tanggal : 03 Juli 2024

Tim Penguji :

1. **Ketua : Aditya Putra Perdana Prasetyo, M.T.**
2. **Sekretaris : Iman Saladin B. Azhar, M.MSI.**
3. **Pembimbing I : Prof. Deris Stiawan, M.T., Ph.D.**
4. **Pembimbing II : Nurul Afifah, M.Kom.**
5. **Penguji : Dr. Ahmad Zarkasi, M.T.**

Mengetahui, 15/7/24
Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERNYATAAN

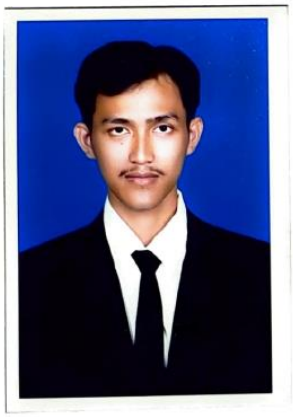
Yang bertanda tangan dibawah ini:

Nama	:	Indra Wicaksono
NIM	:	09011382025128
Judul	:	Deteksi Malware Android Dengan Metode *Reverse Engineering*

Hasil Pengecekan Software *Thenticate/Turnitin*: 6%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.



Palembang, 17 Juli 2024

Indra Wicaksono
NIM. 09011382025128

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji syukur Alhamdulillah penulis panjatkan atas kehadirat Allah SWT yang telah memberikan karunia dan rahmat-Nya, sehingga penulis dapat menyelesaikan penulisan Skripsi yang berjudul "**Deteksi *Malware* Android Dengan Metode *Reverse engineering***".

Pada kesempatan ini penulis ingin mengucapkan terima kasih kepada beberapa pihak atas ide dan saran serta bantuannya dalam menyelesaikan Skripsi ini. Oleh karena itu, penulis ingin mengucapkan rasa syukur kepada Allah SWT dan terima kasih kepada yang terhormat :

1. Kedua orang tua dan keluarga yang telah banyak memberikan do'a dan dukungan serta semangat.
2. Bapak Prof. Dr. Erwin, S.Si., M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
4. Bapak Prof. Deris Stiawan, M.T., Ph.D., IPU., ASEAN Eng. selaku Dosen Pembimbing I Tugas Akhir yang berkenan meluangkan waktu dalam membimbing, memberikan saran dan motivasi untuk penulis dalam menyelesaikan tugas akhir ini.
5. Ibu Nurul Afifah, M.Kom. selaku Dosen Pembimbing II Tugas Akhir yang berkenan meluangkan waktu dalam membimbing, memberikan saran dan motivasi untuk penulis dalam menyelesaikan tugas akhir ini.
6. Ibu Prof. Dr. Ir. Siti Nurmaini, M.T. selaku Dosen Pembimbing Akademik.
7. Mba Renny Virgasari, Pak Yopi serta kak Angga selaku Admin Jurusan Sistem Komputer yang telah membantu dalam mengelola seluruh berkas administrasi.
8. Kedua orang tua, saudara dan keluarga yang telah mendukung penuh.
9. Risky Wahyuni yang telah banyak membantu dalam perkuliahaan ini.
10. Seluruh teman Sistem Komputer 2020.
11. Almamater.

Penulis menyadari bahwa proposal ini masih jauh dari kesempurnaan, oleh karena itu penulis sangat mengharapkan kritik dan saran yang bersifat membangun agar lebih baik lagi dikemudian hari.

Akhir kata dengan segala keterbatasan, penulis berharap semoga Skripsi ini menghasilkan sesuatu yang bermanfaat bagi kita semua khususnya bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung atau pun tidak langsung sebagai sumbangan pikiran dalam peningkatan mutu pembelajaran dan penelitian.

Palembang, Juli 2024
Penulis,

Indra Wicaksono
NIP. 09011382025128

DETEKSI MALWARE ANDROID DENGAN METODE REVERSE ENGINEERING

Indra Wicaksono (09011382025128)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : wicaksonoindra66@gmail.com

ABSTRAK

Smartphone yang digunakan oleh setiap orang terhubung dengan internet setiap waktu. Seorang pengguna tidak menyadari berapa banyak data yang mereka simpan dan tampilkan saat menggunakan beberapa aplikasi. Dengan semakin banyak pengguna android dari waktu ke waktu, android menjadi sasaran para penjahat siber dan menyebabkan peningkatan serangan malware pada perangkat tersebut. *Reverse engineering* merupakan pendekatan yang paling penting dalam menganalisis malware, teknik ini dapat mengekstrak informasi yang cukup lengkap yang diperlukan untuk menganalisis alur logika dari aplikasi tersebut. Penelitian ini akan melakukan *reverse engineering* dan melakukan validasi dengan analisis dinamis menggunakan emulator Android pada beberapa sampel yang ada di repositori malware publik Malware Bazaar. Hasil penelitian menunjukkan bahwa malware sering kali menyamar sebagai aplikasi yang berguna atau normal untuk mengelabui pengguna. Selanjutnya, malware meminta beberapa izin (*permissions*) ke sistem yang seharusnya tidak diperlukan oleh aplikasi tersebut. Izin-izin ini biasanya dimanfaatkan untuk mencuri, mengubah, hingga menghapus data sensitif serta memata-matai pengguna.

Kata kunci: Malware, Android Malware, Reverse Engineering.

ANDROID MALWARE DETECTION WITH REVERSE ENGINEERING METHOD

Indra Wicaksono (09011382025128)
Dept. of Computer System, Faculty of Computer Science, Universitas Sriwijaya
Email : wicaksonoindra66@gmail.com

ABSTRACT

Smartphones used by everyone are connected to the internet at all times. A user is unaware of how much data they store and display while using various applications. With the increasing number of Android users over time, Android has become a target for cybercriminals, leading to an increase in malware attacks on these devices. Reverse engineering is the most crucial approach in analyzing malware; this technique can extract comprehensive information needed to analyze the logic flow of the application. This study will perform reverse engineering and validate it with dynamic analysis using an Android emulator on several samples from the public malware repository Malware Bazaar. The research results show that malware often disguises itself as useful or normal applications to deceive users. Furthermore, malware requests several permissions from the system that should not be required by the application. These permissions are typically exploited to steal, alter, and even delete sensitive data, as well as to spy on users.

Keywords: Malware, Android Malware, Reverse Engineering.

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I
PENDAHULUAN

1.1 Latar Belakang

Smartphone merupakan perangkat *mobile* yang sudah erat disetiap kegiatan sehari-hari manusia. Dengan adanya *Smartphone* yang praktis membuat kegiatan manusia menjadi lebih nyaman dan cepat untuk mendapatkan informasi dan mendapatkan pelayanan dengan jarak jauh secara online [1]. *Smartphone* yang digunakan setiap pengguna tekoneksi dengan data satu hari penuh dan setiap waktu pengguna tidak menyadari berapa banyak data yang mereka simpan dan mereka tampakan saat menggunakan beberapa aplikasi [2].

Salah satu sistem operasi yang paling terkenal pada perangkat *Smartphone* adalah Android, hal ini dikarenakan android merupakan sistem operasi Open Source, sehingga produsen *Smartphone* memiliki kebebasan untuk melakukan modifikasi dan menambahkan aplikasi pre-install sesuai kebutuhan mereka [3]. Dengan banyaknya jumlah pengguna android dari waktu ke waktu, android menjadi sasaran *cyber criminal* dan menjadi penyebab serangan *malware* pada android meningkat [4], [5].

Malware dibuat dengan tujuan untuk melanggar sebuah *Security* policy yang ada pada suatu sistem dan mengancam sebuah data pada aspek yang berhubungan dengan *Confidentiality*, *Integrity* dan *Availability* [6]. *Malware* dapat berada pada suatu sistem dan bersembunyi dalam waktu tertentu tanpa sepengetahuan pemilik sistem [7]. Beberapa tipe *malware* dibuat dengan meniru sebuah aplikasi normal yang biasa digunakan oleh pengguna dan melakukan eksekusi perilaku mencurigakan tanpa kesadaran korban, tipe lainnya adalah *malware* yang menyembunyikan perilaku mencurigakannya agar tidak terdeteksi oleh antivirus dengan menerapkan enkripsi, packing maupun obfuscation pada *source code* mencurigakan [8].

Reverse engineering merupakan pendekatan yang paling penting saat menganalisis *malware*. Teknik *Reverse engineering* dapat mengekstrak informasi yang cukup lengkap yang dapat dikumpulkan untuk menganalisis alur logika dari

aplikasi. *Reverse engineering* membutuhkan kombinasi pengetahuan yang cukup mendalam mengenai sistem komputer dan proses pengembangan aplikasi [9]. Teknik ini juga biasanya digunakan untuk menemukan kerentanan pada suatu aplikasi, membuat rencana serangan dan cracking aplikasi [10].

Pada penelitian [5] penulis melakukan *Reverse engineering* pada tiga sampel tipe aplikasi kalender yaitu iCalendar[.]apk, Kalendar Indonesia[.]apk dan Calendar[.]apk. Sample iCalendar[.]apk merupakan aplikasi malicious sedangkan dua lainnya adalah aplikasi benign. Hasil ekstrasi iCalendar[.]apk menujukkan bahwa aplikasi ini memerlukan izin menerima dan mengirim sms yang seharusnya aplikasi kalender hanya berfungsi untuk menampilkan tanggal saja. Lalu *source code* juga menunjukkan bahwa aplikasi tersebut mengirimkan informasi korban ke nomor premium (1066185829). Hasil ini membuktikan bahwa iCalendar[.]apk merupakan aplikasi yang berbahaya karena mengirimkan data pengguna ke alamat penyerang tanpa izin.

Penelitian [11] melakukan analisis dua aplikasi malicious yang ada pada google playstore yaitu aplikasi transfer uang dengan nama Remit Money Transfer dan aplikasi perekam suara dengan nama *Voice Recording*. Aplikasi Remit Money transfer tidak menunjukkan izin yang mencurigakan sebagai aplikasi transfer uang, namun hasil analisis *Reverse engineering* menunjukkan bahwa *source code* menemukan class yang berfungsi untuk melakukan rekaman audio, cek status ponsel mode *ringing* atau *sleep*, mengubah metode koneksi untuk mengirim data dan fungsi untuk melakukan pencadangan data aplikasi. Lalu pada aplikasi *Voice Recording* yang biasanya hanya memerlukan izin audio dan video saja menghasilkan bahwa aplikasi ini memerlukan izin yang tidak berhubungan dengan audio dan video, aplikasi ini memiliki banyak perilaku mencurigakan yang tidak sesuai dengan fungsi utama aplikasi ini. Hasil analisis dari kedua aplikasi menunjukkan bahwa data pengguna aplikasi tidak aman dan aplikasi banyak menyalahgunakan perangkat dan jaringan. Mengunduh aplikasi dari Google Play Store tidak menjamin bahwa aplikasi tersebut aman.

Penelitian [12] menggunakan sampel botnet dari Android *Malware* Genome Project lalu dilakukan proses *Reverse engineering* dan analsis statis yang

menujukkan botnet mengunduh file konfigurasi XML dari lokasi http://crusewind[.]net. Botnet ini menerima data tambahan untuk mengirim informasi yang diinstall korban ke lokasi server yang telah ditentukan. Botnet ini memiliki fungsi menghapus diri, menghapus SMS hingga mengirim pesan SMS dengan tarif premium yang merugikan korban serta dapat mencuri identitas dan uang korban.

Penelitian [13] melakukan analisis *Reverse engineering* pada sampel com.dotgears.flappybird.apk. Menggunakan tool apktool untuk melakukan dekompilasi lalu mendapatkan file AndroidManifest.xml sehingga kita dapat melihat semua izin yang dibutuhkan aplikasi ini. Banyak izin yang dibutuhkan aplikasi yang seharusnya tidak diperlukan sehingga membuat aplikasi ini tampak mencurigakan. Contohnya adalah izin MOUNT_UNMOUNT_FILESYSTEMS dan KILL_BACKGROUND_PROCESSES. Lalu divalidasi menggunakan virustotal dan menunjukkan bahwa aplikasi tersebut ditandai sebagai *malware* trojan.

Penelitian [14] menggunakan 22 sampel yang didapatkan dari repositori *Malware* APK Android yaitu Koodous dan 30 sampel bebas *malware* yang didapatkan dari Google Play Store. Hasil *Reverse engineering* menunjukkan bahwa file *malware* dan non-*malware* tidak banyak berbeda dari teknik *evasion*. Sebagian besar teknik *evasion* digunakan oleh aplikasi non-*malware*, hal ini membuktikan bahwa sebagian besar teknik *evasion* digunakan untuk tujuan yang tidak berbahaya. Namun pengecualian untuk penggunaan *packer* yang hanya digunakan di aplikasi *malware*. Hasil analisis menunjukkan bahwa tingkat penyebaran *packer* bernilai 9,1% pada *malware*, sedangkan tingkat penyebaran *packer* pada aplikasi non-*malware* adalah 0%.

Penelitian [7] menggunakan sampel dengan nama file best[.]exe dan di analisis dengan metode *Reverse engineering*. Hasil analisis menunjukkan bahwa best[.]exe merupakan *malware* dengan tipe Virus Gen: Variant.Razy, *malware* ini dapat menyembunyikan jejak setelah *download*, mengetahui nama komputer korban, membuat komputer menjadi mode *sleep* dengan waktu yang lama,

membuat task atau proses baru, serta mengirimkan informasi tentang komputer ke penyerang.

Pada penelitian ini akan dilakukan *Reverse engineering* dan divalidasi dengan analisis dinamis dengan emulator android pada beberapa sampel yang ada pada repositori *malware* publik *Malware*-Bazaar yang dirujuk pada penulis [15]. Oleh karena itu, penelitian ini akan diberi judul "**Deteksi *Malware* Android Dengan Metode *Reverse engineering***".

1.2 Perumusan Masalah

Berikut adalah rumusan masalah dalam penulisan tugas akhir ini:

1. Bagaimana cara mendeteksi keberadaan *malware* android?
2. Bagaimana metode infeksi dan aktivitas dari file *malware* android?
3. Bagaimana hasil deteksi *Reverse engineering* dan hasil deteksi Analisis Dinamis?

1.3 Tujuan

Adapun tujuan dari penulisan tugas akhir ini, yaitu:

1. Mendeteksi keberadaan *malware* android menggunakan metode *Reverse engineering*.
2. Memahami cara infeksi dan aktivitas *malware* android.
3. Membandingkan hasil deteksi analisa *Reverse engineering* dengan hasil analisis Dinamis.

1.4 Manfaat

Berikut manfaat dari penulisan tugas akhir ini, yaitu:

1. Dapat mendeteksi keberadaan *malware* android dengan akurat.
2. Dapat mengetahui cara infeksi dan aktivitas dari aplikasi *malware* android.
3. Validasi analisis dinamis membuktikan hasil dari analisis statis dengan metode *Reverse engineering*.

1.5 Batasan Masalah

Berikut batasan masalah dari tugas akhir ini, yaitu:

1. Tidak akan membahas lebih jauh tentang bagaimana aksi pencegahan dan penanganan dari *malware* android.

2. Hanya menganalisis *malware* android.
3. Membahas cara mendeteksi serangan *malware* android.

1.6 Metode Penelitian

Dalam tugas akhir ini akan menggunakan metodologi dan melewati beberapa tahapan sebagai berikut:

1. Tahap Pertama (Studi Pustaka / Literatur)

   Tahapan ini dimulai setelah masalah yang telah dibahas sesuai dengan penelitian sebelumnya yang mengacu banyaknya artikel, paper, jurnal dan buku yang berhubungan dengan penelitian ini yang berjudul "Deteksi *Malware* Android dengan Metode *Reverse engineering*".
2. Tahap Kedua (Perancangan Sistem)

   Tahapan ini merupakan tahapan untuk menentukan perangkat-perangkat yang dibutuhkan pada penelitian, berupa perangkat keras ataupun lunak.
3. Tahap Ketiga (Pengujian)

   Tahapan ketiga ialah pengujian yang sesuai dengan parameter serangan yang ditentukan oleh batasan masalah.
4. Tahap Keempat (Hasil dan Analisa)

   Tahapan keempat mencakup hasil pengujian pada penelitian ini kemudian Hasil penelitian dianalisa untuk mengetahui kelebihan dan kekurangan rancangan penelitian beserta faktor yang mempengaruhi.
5. Tahap Kelima (Kesimpulan dan Saran)

   Tahapan terakhir meliputi kesimpulan dan saran dari hasil studi pustaka dan literatur, perancangan sistem dan analisa pada penelitian. Pada saran berisi poin-poin dari penulis untuk penelitian berikutnya.

1.7 Sistematika Penulisan

Adapun sistematika dalam penulisan tugas akhir ini sebagai berikut:

BAB I PENDAHULUAN

Bab pertama berisi tentang penjabaran secara sistematis yang berupa bahasan atau topik dari penelitian, bab pertama ini meliputi latar belakang masalah, tujuan, manfaat, perumusan masalah, batasan masalah, metodologi yang

digunakan untuk penelitian, serta mengenai sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab kedua ini berisi tentang dasar dan kerangka teori, serta kerangka pikir penelitian, dimana pada bab ini membahas mengenai routing protokol dinamis, konsep route redistribution, metode analisis ANOVA, dan lain sebagainya yang berkaitan langsung terhadap penelitian ini.

BAB III METODOLOGI PENELITIAN

Bab ketiga membahas secara sistematis mengenai proses secara bertahap dan terperinci tentang langkah-langkah yang dilakukan dalam penelitian, guna mencari, mengumpulkan dan menganilisa data yang dihasilkan selama tahap simulasi terhadap skenario route redistribution.

BAB IV HASIL DAN ANALISA

Bab keempat ini membahas tentang hasil pengujian (eksperimen) dari proses yang telah dilakukan. Serta pada bab ini juga analisis akan dilakukan sesuai dengan data yang telah dikumpulkan sebelumnya dari hasil pengujian.

BAB V KESIMPULAN DAN SARAN

Bab kelima atau yang terakhir ini berisi tentang kesimpulan dan saran berdasarkan hasil dan analisa dari penelitian yang telah dilakukan.

DAFTAR PUSTAKA

[1] A. Albakri *et al.*, "Survey on Reverse-Engineering Tools for Android *Mobile* Devices," *Math. Probl. Eng.*, vol. 2022, pp. 1–7, Jan. 2022, doi: 10.1155/2022/4908134.

[2] M. Alrammal, M. Naveed, S. Sallam, and G. Tsaramirsis, "*Malware Analysis*: *Reverse engineering* tools using santuko linux," *Mater. Today Proc.*, vol. 60, pp. 1367–1378, 2022, doi: 10.1016/j.matpr.2021.10.243.

[3] V. Sihag, M. Vardhan, and P. Singh, "A survey of android application and *malware* hardening," *Comput. Sci. Rev.*, vol. 39, p. 100365, Feb. 2021, doi: 10.1016/j.cosrev.2021.100365.

[4] H. Ali *et al.*, "*Security* Hardened and Privacy Preserved Android *Malware* Detection Using Fuzzy Hash of Reverse Engineered *Source code*," *Secur. Commun. Networks*, vol. 2022, pp. 1–11, Sep. 2022, doi: 10.1155/2022/7972230.

[5] M. T. Kyaw, Y. N. Soe, and N. S. Moon Kham, "*Security Analysis* of Android Application by Using *Reverse engineering*," in *Proceedings of 2019 the 9th International Workshop on Computer Science and Engineering*, WCSE, 2019, pp. 171–177. doi: 10.18178/wcse.2019.03.029.

[6] S. Abijah Roseline and S. Geetha, "A comprehensive survey of tools and techniques mitigating computer and *mobile malware* attacks," *Comput. Electr. Eng.*, vol. 92, no. October 2020, p. 107143, Jun. 2021, doi: 10.1016/j.compeleceng.2021.107143.

[7] S. Megira, A. R. Pangesti, and F. W. Wibowo, "*Malware Analysis* and Detection Using *Reverse engineering* Technique," *J. Phys. Conf. Ser.*, vol. 1140, no. 1, p. 012042, Dec. 2018, doi: 10.1088/1742-6596/1140/1/012042.

[8] J. Lim and J. H. Yi, "Structural *Analysis* of packing schemes for extracting hidden codes in *mobile malware*," *EURASIP J. Wirel. Commun. Netw.*, vol. 2016, no. 1, p. 221, Dec. 2016, doi: 10.1186/s13638-016-0720-3.

[9] B. Akram and D. Ogi, "The Making of Indicator of Compromise using *Malware Reverse engineering* Techniques," in *2020 International Conference on ICT for Smart Society (ICISS)*, IEEE, Nov. 2020, pp. 1–6. doi: 10.1109/ICISS50791.2020.9307581.

[10] S. Warda Asher, S. Jan, G. Tsaramirsis, F. Qudus Khan, A. Khalil, and M. Obaidullah, "*Reverse engineering* of *Mobile* Banking Applications," *Comput. Syst. Sci. Eng.*, vol. 38, no. 3, pp. 265–278, 2021, doi: 10.32604/csse.2021.016787.

[11] S. Azam, R. Singh Sumra, B. Shanmugam, K. Cher Yeo, M. Jonokman, and G. Narayana Samy, "*Security Source code Analysis* of Applications in Android OS," *Int. J. Eng. Technol.*, vol. 7, no. 4.15, p. 30, Oct. 2018, doi: 10.14419/ijet.v7i4.15.21366.

[12] Z. Abdullah, M. M. Saudi, and N. B. Anuar, "*Mobile* botnet detection: Proof of concept," in *2014 IEEE 5th Control and Graduate Research Colloquium*, IEEE, Aug. 2014, pp. 257–262. doi: 10.1109/ICSGRC.2014.6908733.

[13] P. Tiwari, G. Tere, and P. Singh, "*Malware* detection in android application by rigorous *Analysis* of decompiled *source code*," in *2016 International Conference on Computing Communication Control and automation (ICCUBEA)*, IEEE, Aug. 2016, pp. 1–6. doi: 10.1109/ICCUBEA.2016.7860070.

[14] J. Hua and A. Hunter, "A Comparative *Analysis* of Properties that May be Used for *Malware* Detection," in *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, IEEE, Nov. 2018, pp. 906–910. doi: 10.1109/UEMCON.2018.8796669.

[15] P. García-Teodoro, J. A. Gómez-Hernández, and A. Abellán-Galera, "Multi-labeling of complex, multi-behavioral *malware* samples," *Comput. Secur.*, vol. 121, p. 102845, Oct. 2022, doi: 10.1016/j.cose.2022.102845.

[16] F. Alswaina and K. Elleithy, "Android *Malware* Family Classification and *Analysis*: Current Status and Future Directions," *Electronics*, vol. 9, no. 6, p. 942, Jun. 2020, doi: 10.3390/electronics9060942.

[17] A. T. Kabakus and I. A. Dogru, "An in-depth *Analysis* of Android *malware* using *hybrid* techniques," *Digit. Investig.*, vol. 24, pp. 25–33, 2018, doi: 10.1016/j.diin.2018.01.001.

[18] T. K. Chawla and A. Kajala, "Transfiguring of an Android App Using *Reverse engineering*," *Int. J. Comput. Sci. Mob. Comput.*, vol. 3, no. 4, pp. 1204–1208, 2014.

[19] M. Salman, Di. Husna, and N. Viani, "Static *Analysis* Method on Portable Executable Files for REMNUX based *Malware* Identification," in *2019 IEEE 10th International Conference on Awareness Science and Technology (iCAST)*, IEEE, Oct. 2019, pp. 1–6. doi: 10.1109/ICAwST.2019.8923331.