ANALISIS RISIKO KEAMANAN DATA WHATSAPP MOD MELALUI PENDEKATAN MALWARE DAN PENGARUHNYA TERHADAP PRIVASI PENGGUNA

Aripin Sihabudin[1)], Talitha Nirmala Neva[2)], Bul Joseph Kon Nyuon[3)], Sahar adnan Abdo Qasem Alselwi[4)], Iwan Setiawan[5)]
[1, 2),3)4)] Teknik Informatika Universitas Nusa Putra
Jl. Raya Cibolang No.21 Cisaat Sukabumi 43152 Indonesia
e-mail: aripin.sihabudin_ti22@nusaputra.ac.id[1)], talitha.nirmala_ti22@nusaputra.ac.id[2)], bul.joseph_ti22@nusaputra.ac.id[3)], Sahar.adnan_ti22@nusaputra.ac.id[4)], iwan.setiawan@nusaputra.ac.id[5)]

* Korespondensi: e-mail: ……..

ABSTRAK

Aplikasi WhatsApp modifikasi, seperti GB WhatsApp, FM WhatsApp, dan WhatsApp Plus, sering digunakan pengguna karena menawarkan fitur tambahan yang tidak tersedia di aplikasi resmi. Namun, aplikasi ini membawa risiko keamanan data dan privasi pengguna yang signifikan. Penelitian ini bertujuan untuk menganalisis ancaman yang ditimbulkan oleh aplikasi modifikasi terhadap privasi dan keamanan data pengguna. Metode yang digunakan mencakup analisis statis melalui VirusTotal dan Mobile Security Framework (MobSF) untuk mendeteksi keberadaan malware, izin berbahaya, serta kerentanan aplikasi. Hasil penelitian menunjukkan bahwa aplikasi modifikasi memiliki tingkat keamanan yang rendah, dengan deteksi malware seperti trojan, perangkat lunak berbahaya, dan modul tambahan tanpa izin pengguna. VirusTotal mengidentifikasi ancaman yang mencakup pencurian data, manipulasi perangkat, dan pengiriman data ke server tidak dikenal. Sementara itu, MobSF mengungkapkan kerentanan seperti Janus vulnerability dan konfigurasi jaringan yang tidak aman, yang memungkinkan serangan man-in-the-middle (MitM). Sebaliknya, aplikasi WhatsApp resmi menunjukkan tingkat keamanan yang jauh lebih tinggi tanpa adanya ancaman yang terdeteksi. Penelitian ini menekankan pentingnya menggunakan aplikasi resmi untuk melindungi privasi dan keamanan pengguna. Edukasi kepada pengguna dan penelitian lebih lanjut tentang risiko aplikasi modifikasi diperlukan untuk meningkatkan kesadaran masyarakat terhadap bahaya yang ditimbulkan.
***Kata Kunci**: WhatsApp Modifikasi, Keamanan Data, Privasi Pengguna, VirusTotal, MobSF*

ABSTRACT

Modified WhatsApp apps, such as GB WhatsApp, FM WhatsApp, and WhatsApp Plus, are often used by users because they offer additional features that are not available in the official app. However, these apps carry significant user privacy and data security risks. This study aims to analyze the threat that modified apps pose to users' privacy and data security. The methods used include static analysis through VirusTotal and Mobile Security Framework (MobSF) to detect the presence of malware, malicious permissions, as well as application vulnerabilities. The results showed that the modified app had a low level of security, with the detection of malware such as trojans, malicious software, and additional modules without user permission. VirusTotal identified threats that included data theft, device manipulation, and sending data to unknown servers. Meanwhile, MobSF revealed vulnerabilities such as the Janus vulnerability and insecure network configurations, which allow man-in-the-middle (MitM) attacks. In contrast, the official WhatsApp app showed a much higher level of security with no threats detected. This study emphasizes the importance of using the official app to protect users' privacy and security. User education and further research on the risks of modified apps are needed to increase public awareness of the dangers they pose.
***Keywords**: WhatsApp Modification, Data Security, User Privacy, VirusTotal, MobSF.*

I. PENDAHULUAN

A. Latar Belakang

Saat ini, teknologi telah berkembang pesat dan telah menjadi bagian penting dari kehidupan manusia. Aplikasi pesan instan atau chatting telah menjadi alat komunikasi yang penting, menggantikan metode konvensional seperti SMS dan panggilan telepon. Aplikasi seperti WhatsApp, Telegram, dan Signal memungkinkan pengguna untuk melakukan panggilan video, berbagi file, dan mengirim pesan secara instan dan murah. Aplikasi chatting telah menjadi kebutuhan sehari-hari bagi jutaan orang di seluruh dunia karena kemudahan dan kecepatan komunikasinya. Namun, seiring dengan perkembangan aplikasi chatting resmi,

muncullah aplikasi-aplikasi modifikasi (Mod) yang menawarkan berbagai fitur tambahan. Mod WhatsApp, seperti GBWhatsApp dan WhatsApp Plus, menarik pengguna dengan fitur-fitur menarik seperti penyesuaian tampilan, menyembunyikan status online, dan mengirim file besar. WhatsApp Mods memberi Anda lebih banyak pilihan daripada aplikasi resmi, penggunaan mods ini membawa beberapa bahaya, terutama yang berkaitan dengan keamanan data dan privasi. WhatsApp Mods dikembangkan oleh pihak ketiga yang tidak selalu mempertimbangkan keamanan pengguna, tidak seperti aplikasi resmi yang memiliki enkripsi end-to-end dan sering diperbarui untuk menutup celah keamanan. Malware yang dapat mencuri data sensitif seperti pesan pribadi, informasi kontak, dan file penting dapat masuk melalui modifikasi ini. Selain itu, ketidakamanan privasi aplikasi Mod memungkinkan pihak ketiga yang tidak bertanggung jawab untuk mengambil data pengguna. Dalam situasi ini, perlu dilakukan analisis bahaya keamanan data untuk penggunaan WhatsApp Mod karena semakin banyak pengguna yang menggunakan aplikasi mod tanpa menyadari bahayanya. Analisis ini diharapkan dapat meningkatkan kesadaran akan ancaman yang mungkin dihadapi dalam menggunakan aplikasi chatting yang dimodifikasi, sekaligus mengingatkan pengguna akan pentingnya menjaga keamanan data mereka.

B. Rumusan Masalah

Penggunaan WhatsApp Mod menimbulkan masalah keamanan dan privasi karena rentan terhadap serangan virus. Penelitian ini melihat beberapa bentuk malware yang dapat membahayakan WhatsApp Mod, pengaruhnya terhadap privasi pengguna, dan pengetahuan pengguna tentang ancaman keamanan.

1) Apa saja jenis malware yang dapat menginfeksi Whatsapp Mod dan bagaimana cara kerjanya untuk mengakses data pengguna?
2) Apa hubungan antara jenis malware yang menyerang Whatsapp Mod dengan tingkat kehilangan privasi yang dialami pengguna?
3) Bagaimana pemahaman dan kesadaran pengguna Whatsapp Mod terhadap risiko keamanan dan privasi mempengaruhi keputusan mereka dalam memilih aplikasi tersebut?

C. Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

1) Umum

Tujuan umum dari penelitian ini adalah untuk menganalisis risiko yang terkait dengan penggunaan aplikasi WhatsApp Mod, terutama berfokus pada kerentanan keamanan yang diperkenalkan oleh malware dan dampaknya terhadap privasi pengguna. Penelitian ini bertujuan untuk memberikan pemahaman yang komprehensif tentang bagaimana malware mengeksploitasi aplikasi yang dimodifikasi dan bagaimana kesadaran pengguna berperan dalam mengurangi risiko privasi.

2) Spesifik

a. Untuk mengidentifikasi jenis-jenis malware yang umumnya menargetkan aplikasi WhatsApp Mod.
b. Untuk mengevaluasi tingkat kesadaran pengguna mengenai risiko keamanan yang terkait dengan penggunaan WhatsApp Mod.
c. Untuk menganalisis hubungan antara jenis malware dan risiko pelanggaran privasi bagi pengguna WhatsApp Mod.
d. Untuk menilai dampak kesadaran pengguna terhadap kemungkinan pelanggaran privasi saat menggunakan WhatsApp Mod.
e. Untuk memberikan rekomendasi kepada pengguna dan pengembang untuk meningkatkan keamanan data dan privasi saat menggunakan atau mengembangkan aplikasi yang dimodifikasi.

D. Manfaat Penelitian

Manfaat dari penelitian ini dapat dibagi menjadi dua kategori, yaitu manfaat teoritis dan manfaat praktis:

1) Manfaat Teoritis

a. Penelitian ini berkontribusi pada pengetahuan yang sudah ada tentang keamanan siber, khususnya dalam konteks aplikasi yang dimodifikasi seperti WhatsApp Mod. Penelitian ini memberikan wawasan tentang bagaimana malware mengeksploitasi aplikasi ini dan bagaimana kesadaran pengguna dapat memengaruhi risiko privasi.
b. Penelitian ini menetapkan kerangka kerja untuk penelitian di masa depan tentang risiko keamanan aplikasi yang dimodifikasi, menawarkan dasar untuk eksplorasi lebih lanjut tentang jenis aplikasi modded lainnya dan kerentanannya.
c. Penelitian ini menyoroti perilaku pengguna dan tingkat kesadaran tentang keamanan siber, yang dapat berguna untuk mengembangkan program pendidikan dan kampanye kesadaran.

2) Manfaat Praktis

a. Bagi Penulis

Penelitian ini memberikan pemahaman yang lebih dalam tentang masalah keamanan siber, khususnya dalam konteks aplikasi seluler dan malware. Penelitian ini meningkatkan kemampuan analisis dan penelitian penulis, yang sangat berharga untuk upaya akademis dan profesional di masa depan.

b. Bagi Institusi Universitas Nusa Putra

Penelitian ini dapat digunakan sebagai referensi untuk penelitian di masa depan di bidang keamanan siber dan teknologi informasi di universitas. Hal ini dapat membantu universitas dalam mengembangkan kurikulum atau lokakarya yang berfokus pada keamanan siber, terutama dalam mendidik mahasiswa tentang risiko penggunaan aplikasi yang dimodifikasi. Temuan dapat dibagikan kepada komunitas akademis yang lebih luas, meningkatkan reputasi universitas dalam bidang penelitian keamanan siber.

c. Bagi Pengguna

Penelitian ini meningkatkan kesadaran di antara para pengguna tentang bahaya menggunakan aplikasi yang tidak resmi dan dimodifikasi seperti WhatsApp Mod. Ini memberikan rekomendasi praktis bagi pengguna untuk melindungi data dan privasi mereka, seperti menghindari penggunaan aplikasi yang dimodifikasi dan berhati-hati tentang izin yang mereka berikan kepada aplikasi.

d. Bagi Pengembang

Penelitian ini menyoroti pentingnya mengembangkan aplikasi yang aman dan risiko yang terkait dengan modifikasi tidak resmi.

II. LANDASAN TEORI

A. Teori Variabel Penelitian

1) Risiko Keamanan Data

Risiko keamanan data mengacu pada potensi ancaman terhadap integritas, kerahasiaan, dan ketersediaan informasi, terutama pada aplikasi komunikasi seperti WhatsApp Mod. Menurut Olaniyi dan Omubo (2023), aplikasi yang dimodifikasi sering kali memiliki celah keamanan karena kurangnya validasi kode dan integrasi pihak ketiga yang tidak aman, yang meningkatkan risiko malware dan ancaman lainnya. Hal ini diperkuat oleh Yadav dan Tiwari (2023), yang menyatakan bahwa enkripsi yang tidak memadai pada platform komunikasi grup dan fitur siaran data meningkatkan potensi eksploitasi informasi sensitif. Metode seperti Anonymous Revocable Identity-Based Broadcast Encryption (ARIBBE) dapat digunakan untuk memberikan keamanan semantik dan melindungi data dari ancaman berbasis plaintext tertentu (IND-CPA). Risiko keamanan yang tinggi ini mempengaruhi perlindungan data pengguna dan sering kali menjadi penyebab utama kebocoran informasi.

2) Privasi Pengguna

Privasi pengguna berkaitan dengan hak individu untuk menjaga keamanan data pribadi mereka selama proses berbagi informasi di platform digital. Olaniyi dan Omubo (2023) mengungkapkan bahwa aplikasi yang dimodifikasi seperti WhatsApp Mod sering kali tidak memiliki kebijakan privasi yang memadai,

sehingga meningkatkan risiko penyalahgunaan data oleh pihak-pihak yang tidak bertanggung jawab. Sejalan dengan itu, Yadav dan Tiwari (2023) menunjukkan pentingnya privasi dalam berbagi data di platform media sosial. Teknologi seperti ARIBBE dirancang untuk menjaga identitas pengguna tetap anonim bahkan untuk penyedia layanan, sambil memastikan bahwa data hanya dapat diakses oleh penerima yang berwenang. Hubungan erat antara risiko keamanan data dan privasi pengguna adalah masalah utama yang dieksplorasi dalam penelitian ini, terutama dalam konteks bagaimana ancaman keamanan dapat secara langsung mempengaruhi perlindungan data dan informasi pribadi.

B. Metode Penelitian Campuran

Metode penelitian campuran adalah pendekatan penelitian yang menggabungkan metode kuantitatif dan kualitatif dalam satu penelitian untuk mendapatkan pemahaman yang lebih komprehensif tentang suatu masalah. Metode ini digunakan ketika peneliti ingin memadukan kekuatan dari kedua pendekatan tersebut, yaitu data numerik dan analisis yang mendalam. Dalam konteks penelitian ini, metode kuantitatif digunakan untuk mengukur tingkat kesadaran pengguna WhatsApp Mod terhadap risiko keamanan data melalui survei atau kuesioner. Sementara itu, metode kualitatif memungkinkan peneliti untuk menggali lebih dalam mengenai pandangan dan pengalaman pengguna terkait dampak privasi dengan wawancara atau analisis deskriptif.

Pendekatan gabungan ini memberikan keuntungan yang signifikan dalam penelitian yang kompleks, seperti menganalisis data keamanan dan privasi pengguna. Data kuantitatif membantu memberikan gambaran statistik tentang tingkat risiko yang dihadapi pengguna, sementara data kualitatif memberikan konteks yang lebih kaya untuk memahami mengapa pengguna tetap memilih WhatsApp Mod meskipun ada risiko yang teridentifikasi. Kombinasi kedua metode ini memungkinkan peneliti untuk mengungkap hubungan antara variabel yang terukur dan perspektif atau pengalaman subjektif pengguna, sehingga hasil penelitian menjadi lebih valid dan relevan.

C. Tinjauan Pustaka (Penelitian Terdahulu)

Studi literatur dilakukan dengan meninjau penelitian dan sumber daya yang relevan tentang risiko keamanan data pada aplikasi yang dimodifikasi, khususnya WhatsApp Mod, serta dampak malware terhadap privasi pengguna dan kesadaran keamanan digital. Beberapa penelitian yang dibahas yang relevan antara lain:

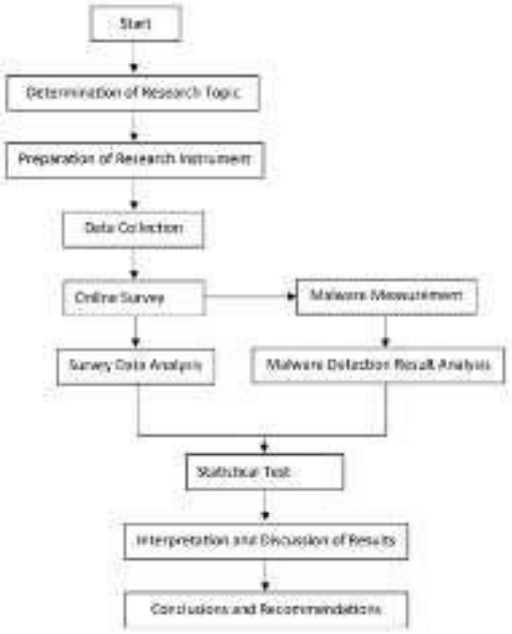
Pertama, penelitian yang dilakukan oleh Fahmy Trimuti Saputra, Banu Santoso, Jeki Kuswanto, M. Abdul Ghofur (2021) mahasiswa Universitas Amikom Yogyakarta dengan judul: "Analisis Keamanan Informasi Kesadaran Pengguna Whatsapp Mod dengan Metode Analisis Statis dan Metode Kuantitatif". Penelitian ini menghasilkan analisis menggunakan VirusTotal, terdeteksi bahwa ketiga WhatsApp Mod yang digunakan sebagai bahan pendukung penelitian ini mengandung setidaknya dua ancaman yang dapat membahayakan pengguna dan perangkat yang digunakan, pada hasil analisis menggunakan MobSF pada Tabel Perizinan, ketiga aplikasi tersebut banyak mendapatkan status Dangerous atau Berbahaya pada perizinan yang ada pada aplikasi tersebut, sedangkan pada tabel analisis kode didapatkan hasil bahwa isu yang menjadi kerentanan aplikasi WhatsApp Mod tidak sesuai dengan standar yang ada. Persamaan penelitian tersebut dengan penelitian saat ini adalah menganalisa data dan keamanan pengguna pada whatsapp mod, sedangkan perbedaannya adalah penelitian saat ini hanya menggunakan satu jenis whatsapp mod.

Kedua, penelitian yang dilakukan oleh Imam Himawan, Kevin Septianzah, Irawan Setiadi (2022) mahasiswa dari Universitas Indraprasta PGRI dengan judul: "Analisis Keamanan Informasi Malware Terhadap Aplikasi APK dengan Metode Static Analysis Menggunakan MobSF". Penelitian ini menghasilkan proses analisis yang dilakukan pada aplikasi sistem pakar pencernaan android menunjukkan bahwa tingkat keamanan masih relatif sama, adanya celah keamanan yang ditemukan dapat menjadi security awareness bagi pengguna aplikasi. Perbedaannya adalah penelitian ini melakukan analisis pada file informasi aplikasi yang memiliki APK (Application Package File).

Ketiga, penelitian yang dilakukan oleh Muhammad Rifqi Ramadhani dan Ahmad Raf'ie Pratama (2020) mahasiswa Universitas Islam Indonesia dengan judul: "Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Indonesia". Penelitian ini menghasilkan tingkat kesadaran pengguna media sosial di Indonesia dipengaruhi oleh usia dan domisili pengguna. Persamaan penelitian tersebut dengan penelitian

saat ini adalah kesadaran pengguna media sosial. Perbedaannya adalah penelitian saat ini hanya menggunakan satu media sosial yaitu whatsapp.

D. Alur Penelitian



Gambar 1. Tahapan Penelitian

Penelitian ini dimulai dengan identifikasi masalah dan tujuan, yaitu meneliti dampak terhadap privasi pengguna dan ancaman keamanan data pada WhatsApp Mod dengan menggunakan metodologi virus. Setelah pemilihan masalah, kuesioner untuk survei online dan alat analisis malware disiapkan untuk membangun instrumen studi. Pengukuran malware dan kuesioner digunakan dalam prosedur pengumpulan data. Sementara temuan pengukuran malware dikategorikan menurut kategori ancaman yang ditemukan, data survei dari responden dianalisis secara statistik. Setelah interpretasi gabungan mereka, kedua temuan ini menghasilkan kesimpulan dan saran yang berkaitan dengan tujuan penelitian. Pembuatan laporan komprehensif yang didasarkan pada hasil utama menandai akhir dari penelitian ini.

E. Variabel Penelitian

Variabel penelitian ini terdiri dari:

1) Variabel Eksogen (Variabel Bebas): Risiko keamanan data WhatsApp Mod melalui pendekatan malware.
2) Variabel Endogen (Variabel Terikat): Privasi pengguna, diukur berdasarkan persepsi mereka terhadap dampak risiko keamanan dari penggunaan WhatsApp Mod.

F. Hipotesis Penelitian

Sebelum melakukan analisis lebih lanjut, penulis merumuskan hipotesis untuk membuktikan signifikansi hubungan antara faktor atau variabel laten, seperti keamanan data (X), dan variabel privasi pengguna (Y). Hipotesis ini disusun berdasarkan indikator-indikator yang relevan untuk menguji pengaruh masing-masing variabel. Hipotesis yang dirumuskan adalah sebagai berikut:

1) Tidak terdapat hubungan yang signifikan antara tingkat keamanan data pada WhatsApp Mod (X) dengan privasi pengguna (Y).
2) Terdapat hubungan positif/negatif yang signifikan antara tingkat keamanan data pada WhatsApp Mod (X) dengan privasi pengguna (Y).

a. Pengujian Reliabilitas dan Validitas

Pengujian reliabilitas adalah proses untuk memastikan bahwa instrumen penelitian, seperti kuesioner, menghasilkan data yang konsisten dan dapat diandalkan ketika digunakan dalam situasi yang berbeda atau pada waktu yang berbeda. Pengujian ini sering dilakukan dengan menggunakan nilai

Cronbach's Alpha, di mana nilai di atas 0.6 umumnya dianggap menunjukkan tingkat reliabilitas yang baik. Jika nilai reliabilitas tinggi, maka instrumen tersebut dianggap mampu mengukur variabel penelitian secara konsisten.

Pengujian validitas, di sisi lain, bertujuan untuk memastikan bahwa instrumen benar-benar mengukur apa yang ingin diukur. Pengujian ini biasanya dilakukan dengan menggunakan metode validitas isi atau validitas konstruk. Validitas isi menguji sejauh mana pertanyaan-pertanyaan dalam kuesioner mencakup semua aspek dari variabel yang diteliti. Validitas yang baik memastikan bahwa data yang diperoleh relevan dan mendukung tujuan penelitian.

b. Analisis Deskriptif dan Tabel Kategorisasi

Analisis deskriptif adalah metode yang digunakan untuk menganalisis data dengan cara mendeskripsikan atau menggambarkan karakteristik utama data yang terkumpul. Analisis ini memberikan ringkasan statistik seperti mean, median, modus, standar deviasi, dan distribusi frekuensi. Tujuannya adalah untuk memberikan gambaran umum mengenai data sebelum dilakukan analisis yang lebih mendalam, seperti korelasi atau regresi.

Tabel kategorisasi digunakan untuk mengelompokkan data ke dalam kategori tertentu berdasarkan skala atau kriteria yang telah ditentukan. Sebagai contoh, tingkat kesadaran pengguna terhadap keamanan data dapat dikategorikan menjadi rendah, sedang, dan tinggi berdasarkan rentang nilai tertentu. Tabel ini memudahkan interpretasi data dengan memberikan visualisasi yang jelas mengenai sebaran responden di setiap kategori. Hal ini sangat membantu dalam memahami pola atau tren dalam data serta mendukung analisis lebih lanjut.

c. Uji Normalitas, Linieritas, Analisis Inferensial

Uji normalitas digunakan untuk menguji apakah data berdistribusi normal dengan cara menganalisis nilai skewness dan kurtosis dari variabel-variabel penelitian yang penting untuk menentukan penggunaan metode analisis statistik parametrik atau non-parametrik. Uji linearitas bertujuan untuk mengetahui apakah hubungan antara variabel independen dan dependen bersifat linear, biasanya melalui analisis ANOVA, dan jika hubungan tidak linear maka akan digunakan metode non parametrik dalam analisis inferensial. Analisis inferensial dilakukan untuk menguji hipotesis dan menentukan kekuatan dan arah hubungan antar variabel dengan menggunakan koefisien korelasi yang menunjukkan signifikansi hubungan tersebut. Sementara itu, analisis regresi sederhana digunakan untuk mengukur pengaruh variabel independen terhadap variabel dependen melalui persamaan regresi, dimana nilai koefisien regresi menunjukkan perubahan variabel dependen berdasarkan perubahan variabel independen, dan nilai R^2 menunjukkan kontribusi variabel independen terhadap variabel dependen, dengan pengaruh sisanya berasal dari faktor lain di luar penelitian.

III. Metode Penelitian

A. Desain Penelitian

Penelitian ini menggunakan pendekatan metode campuran, menggabungkan kuantitatif dan kualitatif untuk menyelidiki kerentanan keamanan data di WhatsApp Mod dan dampaknya terhadap privasi pengguna. Penelitian ini merupakan penelitian deskriptif yang berfokus pada jenis-jenis malware yang ada di aplikasi yang dimodifikasi, kesadaran pengguna akan risikonya, dan korelasi antara risiko malware dan masalah privasi. Ruang lingkup penelitian ini terbatas pada pengguna yang secara aktif menggunakan WhatsApp Mod. Analisis akan menggunakan statistik deskriptif dan analisis korelasi untuk mengevaluasi tujuan penelitian.

B. Sampel dan Populasi

Strategi pengambilan sampel yang digunakan dalam penelitian ini adalah survei online yang disampaikan kepada pengguna WhatsApp di Indonesia melalui Google Form. Populasi dalam penelitian ini sebanyak 50 responden yang dipilih dengan kriteria utama adalah pengguna yang telah menggunakan program WhatsApp Mod.

C. Metode Pengumpulan Data

Metode Pengumpulan Data merupakan langkah penting dalam penelitian untuk mengumpulkan informasi atau data yang relevan untuk menjawab pertanyaan penelitian dan mencapai tujuan penelitian.

1) Kuesioner

Kuesioner merupakan salah satu metode pengumpulan data yang dilakukan dengan cara menyampaikan sejumlah pertanyaan kepada responden untuk dijawabnya. Metode ini sangat efisien dan efektif, terutama bila peneliti telah mengetahui dengan jelas variabel yang akan diukur dan informasi yang ingin diperoleh dari responden.

2) Data Responden

Sampel terdiri dari 50 responden yang dipilih dengan menggunakan pendekatan purposive sampling, dengan kriteria utama adalah pengguna yang telah menggunakan program WhatsApp Mod. Hasil survei menunjukkan bahwa mayoritas responden adalah laki-laki (60%) dan perempuan (40%). Dalam hal usia, sebagian besar responden berada dalam rentang usia 18-24 tahun, yaitu 92%, diikuti oleh mereka yang berusia di bawah 18 tahun sebanyak 2%, dan kelompok yang lebih kecil yaitu 4% dalam rentang usia 25-34 tahun. Mengenai pekerjaan, sebagian besar responden adalah pelajar (68%), sementara yang lainnya bekerja sebagai karyawan swasta (12%), wiraswasta (4%), atau termasuk dalam kategori lainnya (16%). Selain itu, responden yang pernah menggunakan WhatsApp Mod, baik secara aktif maupun di masa lalu, membagikan pengalaman mereka tentang risiko yang dirasakan dan masalah privasi yang terkait dengan aplikasi tersebut. Penulis menggunakan simple random sampling untuk metode pengumpulan data.

3) Simple Random Sampling

Simple Random Sampling adalah metode pengambilan sampel di mana setiap anggota populasi memiliki kesempatan yang sama untuk dipilih. Metode ini dianggap sebagai salah satu yang paling dasar dan umum digunakan dalam statistik.

4) SPSS

SPSS (Statistical Package for the Social Sciences) adalah perangkat lunak statistik yang banyak digunakan untuk analisis data dan pemrosesan statistik. SPSS memudahkan pengguna untuk memproses data secara efisien melalui berbagai fitur, termasuk Analisis Deskriptif, Uji Statistik, Pengolahan Data, Visualisasi Data. SPSS sangat terkenal untuk antarmuka grafis yang ramah pengguna, membuatnya lebih mudah diakses oleh mereka yang tidak memiliki latar belakang yang kuat yang kuat dalam statistik atau pemrograman.

D. Analisis Statis

Analisis statis adalah metode evaluasi keamanan aplikasi yang dilakukan tanpa menjalankan aplikasi. Prosesnya melibatkan pemeriksaan langsung terhadap file atau kode sumber aplikasi untuk mengidentifikasi potensi ancaman atau kerentanan keamanan. Analisis statis memungkinkan peneliti untuk mengevaluasi struktur aplikasi, izin yang diminta, dan integrasi kode tanpa risiko memicu perilaku berbahaya dari aplikasi. Teknik ini sangat berguna untuk memahami bagaimana aplikasi dirancang dan mengidentifikasi kelemahan pada tingkat kode.

Penggunaan gabungan VirusTotal dan MobSF memberikan pendekatan yang komprehensif untuk mengevaluasi risiko keamanan data di WhatsApp Mod. VirusTotal menyediakan deteksi ancaman malware berbasis luas, sementara MobSF menyediakan analisis terperinci pada tingkat kode dan izin aplikasi. Pendekatan ini tidak hanya membantu memahami risiko keamanan yang dihadapi pengguna, tetapi juga memberikan dasar untuk merekomendasikan langkah-langkah mitigasi yang lebih efektif.

1) VirusTotal

VirusTotal digunakan untuk mendeteksi keberadaan malware atau ancaman keamanan lainnya pada file APK WhatsApp Mod. Prosesnya melibatkan pemindaian file menggunakan berbagai mesin antivirus secara bersamaan untuk mengidentifikasi jenis ancaman, tingkat keparahannya, dan potensi dampaknya terhadap perangkat pengguna. Hasil dari *VirusTotal* memberikan gambaran awal tentang ancaman keamanan yang mungkin terkandung di dalam aplikasi.

2) MobSF

MobSF digunakan untuk analisis keamanan yang lebih mendalam melalui metode statis. Ini memeriksa berbagai aspek aplikasi, seperti kode sumber, izin aplikasi, penggunaan API, dan potensi lainnya kerentanan lainnya. Dengan MobSF, peneliti dapat mengidentifikasi komponen yang berisiko diserang, seperti akses yang tidak sah akses tidak sah ke data pengguna atau integrasi kode yang lemah. Hasil analisis

ini membantu mengungkap berbagai celah keamanan yang dapat dieksploitasi oleh pihak-pihak yang tidak bertanggung jawab.

IV. Analisis Data dan Pembahasan

A. Hasil Analisis Data

1) Pengujian Reliabilitas dan Validitas

Tahapan ini dilakukan untuk memastikan bahwa instrumen penelitian, termasuk kuesioner dan alat ukur malware yang dapat dilihat pada lampiran tabel A1, memiliki tingkat validitas dan reliabilitas yang tinggi. Data hasil survei divalidasi dengan menggunakan uji validitas dan reliabilitas.

No	R Calculate	R Tabel	DESCRIPTION
1	.606**	0,273	VALID
2	.629**	0,273	VALID
3	.643**	0,273	VALID
4	.603**	0,273	VALID
5	.610**	0,273	VALID
6	.612**	0,273	VALID
7	.296*	0,273	VALID
8	.410**	0,273	VALID
9	0,228	0,273	NOT VALID
10	0,129	0,273	NOT VALID

Tabel 1. Tabel Hasil Uji Validitas

Reliability Statistics	
Cronbach's Alpha	N of Items
0,669	10

Item-Total Statistics				
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
X01	32,8980	37,885	0,434	0,623
X02	32,3878	36,659	0,442	0,620
X03	31,6122	37,867	0,492	0,612
X04	31,5510	38,794	0,446	0,622
X05	31,3878	38,159	0,443	0,622
X06	32,7143	36,667	0,426	0,624
X07	31,5918	44,872	0,104	0,687
X08	32,0000	42,792	0,244	0,661
X09	30,8163	46,653	0,129	0,673
X10	30,7959	47,707	0,019	0,685

Tabel 2. Tabel Hasil Uji Reliabilitas

2) Analisis Deskriptif dan Tabel Kategorisasi

Data yang dikumpulkan dianalisis secara deskriptif untuk memberikan gambaran umum mengenai karakteristik responden dan persepsi mereka terhadap keamanan dan privasi data. Data ini kemudian dikategorikan untuk untuk memudahkan analisis hubungan antar variabel.

a. Analisis Deskriptif

Pengolahan data untuk mencari ukuran-ukuran statistik dasar, seperti: mean, median, range, dan varians, skewness dan kurtosis untuk variabel X dan variabel Y.

Descriptives

	Statistic	Std. Error

whatsapp mod data security risk through malware approach and its effects	**Mean**		**22.4600**	.83505
	95% Confidence Interval for Mean	Lower Bound	20.7819	
		Upper Bound	24.1381	
	5% Trimmed Mean		22.5111	
	Median		22.0000	
	Variance		34.866	
	Std. Deviation		**5.90472**	
	Minimum		9.00	
	Maximum		35.00	
	Range		26.00	
	Interquartile Range		7.25	
	Skewness		.031	.337
	Kurtosis		-.064	.662
user privacy	**Mean**		**12.9200**	.26161
	95% Confidence Interval for Mean	Lower Bound	12.3943	
		Upper Bound	13.4457	
	5% Trimmed Mean		13.0556	
	Median		13.0000	
	Variance		3.422	
	Std. Deviation		**1.84988**	
	Minimum		7.00	
	Maximum		15.00	
	Range		8.00	
	Interquartile Range		3.00	
	Skewness		-.866	.337
	Kurtosis		.769	.662

Tabel 3. Tabel Analisis Deskriptif

b. Tabel Kategorisasi

Berdasarkan nilai rata-rata (μ) dan standar deviasi (σ), variabel keamanan data dan privasi pengguna dikelompokkan ke dalam tiga kategori yaitu rendah, sedang, dan tinggi. Hasil kategorisasi menunjukkan bahwa 37% responden berada pada kategori sedang untuk tingkat risiko keamanan data, sementara hanya 7% yang berada pada kategori tinggi. Sementara itu, untuk privasi pengguna, mayoritas responden (27%) berada dalam kategori sedang, namun 13% responden menilai privasi mereka sangat penting, yang mencerminkan kepedulian yang cukup tinggi terhadap perlindungan informasi pribadi. Temuan ini menunjukkan bahwa meskipun sebagian besar responden menyadari risiko keamanan data, mereka tetap memprioritaskan privasi dalam penggunaan WhatsApp Mod.

Category Limits	Interval	Frequency	Percentage	Description
X < (μ-1,0σ)	X ≤ 16,5553	6	6%	Low
(μ-1,0σ) ≤ X < (μ + 1,0σ)	16,5553 ≤ X ≥ 28,3647	37	37%	Medium
(μ + 1,0σ) ≤ X	28,3647 ≤ X	7	7%	High
TOTAL		50	50%	

Tabel 4. Kategorisasi risiko keamanan data whatsapp mod melalui pendekatan malware dan efeknya Tabel

Category Limits	Interval	Frequency	Percentage	Description
X < (μ-1,0σ)	X ≤ 11,07012	10	10%	Low
(μ-1,0σ) ≤ X < (μ + 1,0σ)	11,07012 ≤ X ≥ 14,76988	27	27%	Medium

(μ + 1,0σ) ≤ X	14,76988 ≤ X	13	13%	High
TOTAL		50	50%	

Tabel 5. Tabel kategorisasi privasi pengguna

3) Uji Normalitas, Uji Linieritas, Analisis Inferensial

a. Uji Normalitas

Dilakukan untuk mengetahui apakah data terdistribusi secara normal. Berdasarkan tabel deskriptif, skewness (0,031 untuk X, -0,866 untuk Y) dan kurtosis (0,064 untuk X, 0,769 untuk Y) menunjukkan distribusi yang tidak normal.

b. Uji Linieritas

Hasil uji linearitas (ANOVA) menunjukkan bahwa hubungan antara X dan Y tidak linear, sehingga analisis inferensial menggunakan metode non parametrik, yaitu korelasi Rank Spearman.

			Sum of Squares	df	Mean Square	F	Sig.
user privacy * whatsapp mod data security risk through malware approach and its effects	Between Groups	(Combined)	101.863	20	5.093	2.244	.023
		Linearity	32.281	1	32.281	14.224	.001
		Deviation from Linearity	69.582	19	3.662	1.614	.120
	Within Groups		65.817	29	2.270		
	Total		167.680	49			

Tabel .6. Tabel ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	32.281	1	32.281	11.444	.001[b]
	Residual	135.399	48	2.821		
	Total	167.680	49			

Tabel.7. Tabel ANOVA untuk Nilai Signifikansi

Berdasarkan output di atas, diketahui bahwa nilai signifikansi (Sig.) sebesar 0,001 < 0,05, sehingga dapat disimpulkan bahwa H0 ditolak dan Ha diterima, yang berarti bahwa "Terdapat pengaruh risiko keamanan data whatsapp mod melalui pendekatan malware dan dampaknya (X) terhadap privasi pengguna (Y)".

c. Analisis Inferensial

Spearman's rho	whatsapp mod data security risk through malware approach and its effects	Correlation Coefficient	1.000	.328*
		Sig. (2-tailed)	.	.020
		N	50	50
	user privacy	Correlation Coefficient	.328*	1.000
		Sig. (2-tailed)	.020	.
		N	50	50

Tabel 8. Tabel Uji Korelasi Rank Spearman

Dari hasil korelasi diperoleh nilai koefisien korelasi (r) = 0,328 yang menunjukkan adanya hubungan positif dengan kekuatan hubungan yang cukup kuat. Nilai signifikansi (p-value) = 0,020 < 0,05 sehingga hipotesis nol (H0) ditolak, dan hipotesis alternatif (Ha) diterima. Artinya terdapat hubungan yang signifikan antara tingkat keamanan data pada whatsapp mod dengan privasi pengguna.

d. Simple Linear Regression

		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	t	Sig.
1	(Constant)	9.833	.943		10.427	.000

whatsapp mod data security risk through malware approach and its effects	.137	.041	.439	3.383	.001

Tabel 9. Tabel Koefisien

a = angka konstan dari koefisien yang tidak terstandarisasi. Dalam hal ini adalah 9,833.
Angka ini merupakan angka konstanta yang berarti bahwa jika tidak ada risiko keamanan data whatsapp mod melalui pendekatan malware dan dampaknya (X), maka nilai privasi pengguna (Y) adalah 9.833.
b = angka koefisien regresi. Nilainya sebesar 0,137. Angka tersebut berarti bahwa setiap kenaikan 1% tingkat risiko keamanan data whatsapp mod melalui pendekatan malware dan dampaknya (X), maka privasi pengguna (Y) akan meningkat sebesar 0,137.
Karena nilai koefisien regresi bertanda plus (+), maka dapat dikatakan bahwa risiko keamanan data whatsapp mod melalui pendekatan malware dan dampaknya (X) berpengaruh positif terhadap privasi pengguna (Y). Sehingga persamaan regresinya adalah Y = 9,833 + 0,173 X

B. Hasil Analisis Statis

1. VirusTotal

a. GB WhatsApp v31.15

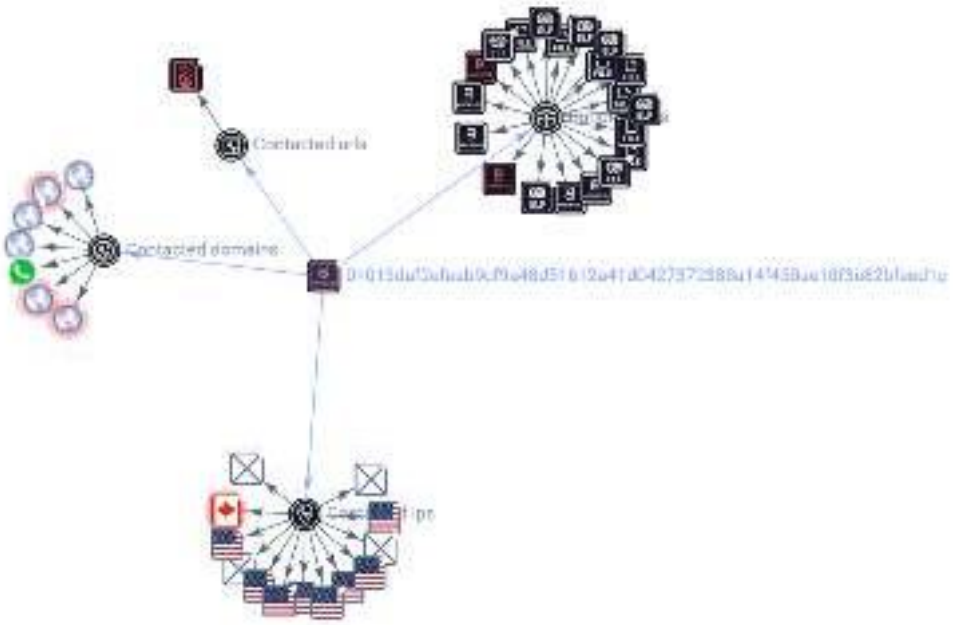
Untuk memastikan analisisnya akurat dan sesuai dengan kondisi saat ini, penulis mengunduh versi terbaru dari aplikasi ini. Karena versi terbaru memiliki peningkatan fitur terbaru dan potensi kerentanan yang mungkin tidak ada di versi sebelumnya, menggunakannya kemungkinan besar akan menghasilkan hasil deteksi yang lebih andal dari produk keamanan seperti VirusTotal. Versi 31.15 dari perangkat lunak WhatsApp GB yang diteliti dirilis pada 5 Desember 2024, oleh pengembang apk unduhan WhatsApp GB. Semua bahasa didukung oleh aplikasi berukuran 88 megabyte tersebut.

Gambar 2. Informasi GB WhatsApp v31.15

No	Nama Vendor	Jenis Deteksi	Deskripsi Ancaman	Dampak Potensial Pada Pengguna
1	BitDefenderFalx	Android.Riskware.Agent.NGH	Aplikasi berisiko yang dapat menyebabkan kerentanan keamanan.	Pencurian data pribadi dan potensi penyalahgunaan perangkat.
2	DrWeb	Android.Click.1751	Malware yang dapat mengarahkan pengguna ke situs web berbahaya tanpa izin.	Risiko phishing yang dapat mencuri kredensial pengguna.
3	Ikarus	PUA.AVE.Agent	Risiko phishing yang dapat mencuri kredensial pengguna Potensi aplikasi yang tidak diinginkan yang dapat menyebabkan masalah keamanan.	Menyebabkan perangkat melambat dan menampilkan iklan yang tidak sah.
4	Symantec Mobile Insight	Other:Android.Reputation.2	Deteksi berdasarkan reputasi aplikasi	Aplikasi mungkin mengandung

			yang rendah di komunitas keamanan.	kode berbahaya yang tidak terdeteksi sepenuhnya.

Tabel 10. Laporan Deteksi Vendor Keamanan dari GB WhatsApp



Gambar 3. Ringkasan Grafik GB WhatsApp

GB WhatsApp ditemukan terlibat dalam sejumlah praktik yang dipertanyakan oleh VirusTotal, termasuk:

- Menggunakan teknik pemrograman yang mengubah perilaku program secara real time, yang sering digunakan oleh malware untuk menyembunyikan aktivitas berbahaya.
- Tanpa disadari pengguna, program tersebut dapat mengirim pesan SMS.
- Aplikasi ini menggunakan GPS untuk menentukan posisi perangkat.
- Untuk mencegah alat keamanan mendeteksinya, kode aplikasi disamarkan.
- GB Beberapa domain dan URL, termasuk apisgoogle.org dan google.apisgoogle.org, yang meniru domain resmi Google dan digunakan untuk upaya phishing atau pencurian data pengguna, dicoba dihubungi oleh WhatsApp.
- Aplikasi ini mencoba menghubungi banyak alamat IP, termasuk yang terdaftar di Amerika Serikat. Meskipun ada kemungkinan aplikasi akan mentransfer data ke server yang tidak dikenal, beberapa di antaranya terhubung ke infrastruktur CDN (Content Delivery Network) yang valid.
- APK ini hadir dengan sekitar 198 file, termasuk banyak file classes.dex yang menyimpan kode eksekusi untuk aplikasi. Vendor keamanan mengidentifikasi beberapa file ini - seperti classes2.dex dan classes6.dex - sebagai file yang mencurigakan.

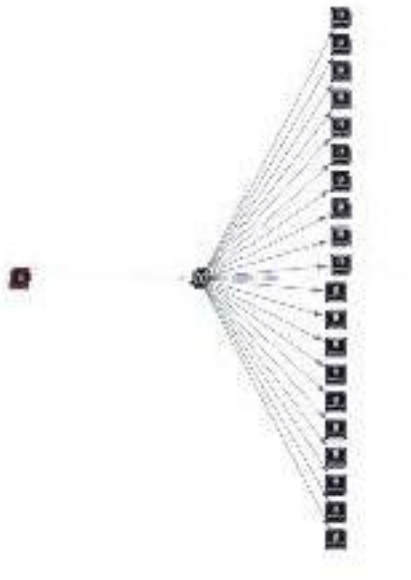
b. FM WhatsApp v10.10

Dikembangkan oleh Fouad Mods, versi terbaru WhatsApp FM adalah v10.10. Perangkat lunak ini berukuran 79 MB dan membutuhkan Android 4.4 atau yang lebih baru untuk menjalankannya. Untuk memastikan bahwa analisis ini menggunakan versi terbaru dari program ini, program ini telah diperbarui untuk ketiga kalinya pada tanggal 13 Januari 2025.

Gambar.4. Informasi FM WhatsApp v10.10

No	Nama Vendor	Jenis Deteksi	Deskripsi Ancaman	Dampak Potensial Pada Pengguna
1	Avast-Mobile	Android:Evo-gen [Trj]	Trojan umum yang dapat mencuri data pribadi pengguna.	Pencurian data, akses ke pesan pribadi, dan kendali jarak jauh atas perangkat.
2	Avira	ANDROID/AVE.Evo.ybkjdz	Malware yang berpotensi menyebabkan kerentanan pada perangkat.	Membuka celah keamanan yang memungkinkan pengunduhan kode berbahaya.
3	Cynet	Malicious (score: 99)	File dianggap berbahaya dengan skor deteksi yang tinggi.	Risiko infeksi malware yang dapat mencuri informasi sensitif pengguna File dianggap berbahaya dengan skor deteksi tinggi.
4	DrWeb	Android.Packed.57146	Malware yang dikemas untuk menghindari deteksi oleh alat keamanan.	Menginstal malware tersembunyi yang dapat mengganggu kinerja perangkat.
5	Ikarus	AndroidOS.BankBot	Trojan perbankan yang dirancang untuk mencuri kredensial keuangan pengguna.	Pencurian informasi keuangan yang dapat digunakan untuk penipuan.
6	Kaspersky	HEUR:Trojan.AndroidOS.Triada.ga	Triada Trojan yang dapat menginstal modul tambahan tanpa izin pengguna.	Pemasangan modul berbahaya dan perangkat kontrol tanpa persetujuan.
7	WithSecure	PotentialRisk.PUA/ANDR.Packed.FSTJ.Gen	Aplikasi yang berpotensi tidak aman dan dapat menyebabkan risiko keamanan.	Risiko terhadap privasi dan potensi pencurian data.

Tabel.11. Laporan Deteksi Vendor Keamanan dari FM WhatsApp



Gambar.5. Ringkasan Grafik FM Whatsapp

VirusTotal mengidentifikasi aktivitas mencurigakan:

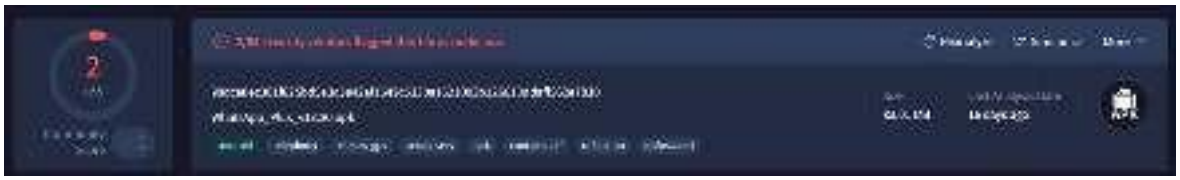
- FM. WhatsApp mengintegrasikan fitur-fitur yang biasa terlihat di file Windows, yang unik untuk aplikasi Android. Ini mengimplikasikan bahwa mungkin ada program berbahaya yang terinstal.

- Malware menggunakan kode perangkat lunak yang disamarkan untuk menghindari deteksi. Virus ini terkenal karena memasang modul tambahan tanpa sepengetahuan pengguna, mengambil alih perangkat, dan mengumpulkan informasi pribadi.

- Paket berisi sekitar 99 file yang dibundel, termasuk file XML dan classes.dex. Virus ini sering kali menargetkan file classes.dex, yang berisi kode yang dapat dieksekusi.

c. WhatsApp Plus v18.30

Aplikasi yang dianalisis adalah versi terbaru yang dikembangkan oleh pengembang pihak ketiga. Aplikasi ini memiliki ukuran sekitar 83 megabyte. Analisis dilakukan pada versi yang baru saja diperbarui untuk memastikan hasilnya mencerminkan kondisi aplikasi terkini.



Gambar.6. Informasi WhatsApp Plus v18.30

No	Nama Vendor	Jenis Deteksi	Deskripsi Ancaman	Dampak Potensial Pada Pengguna
1	BitDefenderFalx	Android.Riskware.TestKey.rA	Aplikasi yang ditandai sebagai riskware, yang	Potensi keamanan yang rendah karena aplikasi

			menggunakan kunci pengembang tes.	mungkin belum diverifikasi dengan benar.
2	Symantec Mobile Insight	AppRisk:Generisk	Potensi keamanan yang rendah karena aplikasi mungkin belum diverifikasi dengan benar Risiko aplikasi umum dengan kepercayaan yang rendah pada komunitas keamanan.	Aplikasi mungkin berisi kode berbahaya yang tidak terdeteksi sepenuhnya.

Tabel.12. Laporan Deteksi Vendor Keamanan dari WhatsApp Plus

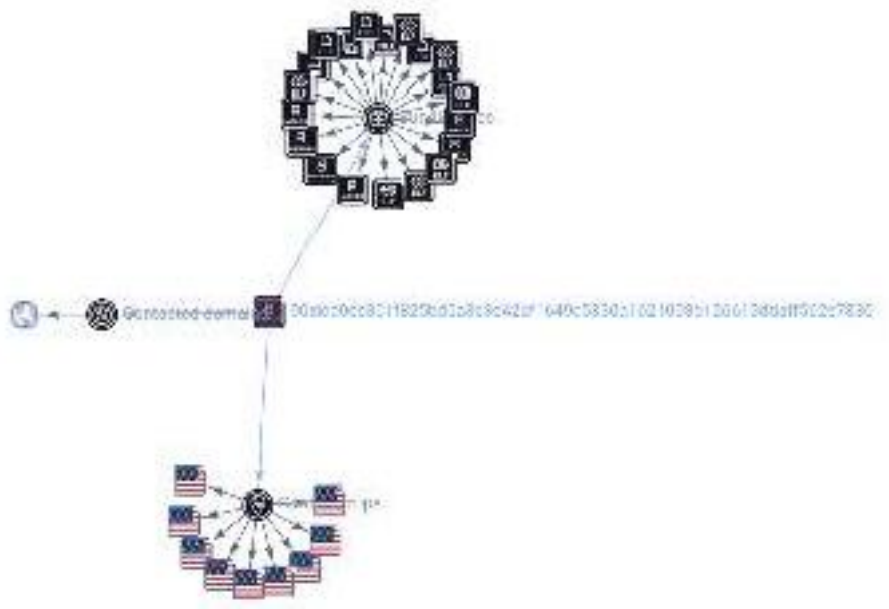


Figure.7. Ringkasan Grafik WhatsApp Plus

VirusTotal mendeteksi banyak operasi meragukan yang dilakukan oleh WhatsApp Plus v18.30, termasuk:

- Menggunakan teknik pemrograman untuk mengubah perilaku aplikasi pada saat runtime, yang sering digunakan untuk menyembunyikan aktivitas berbahaya.
- Mengirim Dapat mengirim pesan SMS tanpa sepengetahuan pengguna.
- Memeriksa posisi perangkat menggunakan GPS.
- Kode aplikasi telah disamarkan untuk menghindari deteksi oleh alat keamanan.
- Aplikasi ini terdiri dari 197 file yang dipaketkan, termasuk banyak file classes.dex yang berisi kode eksekusi program. Beberapa file ini mungkin berisi kode berbahaya yang sulit dideteksi.

2. MobSF

a. GB WhatsApp

Hasil pemindaian menunjukkan bahwa program GB WhatsApp v31.15 memiliki risiko keamanan yang signifikan. Skor keamanan 50/100 menyiratkan bahwa aplikasi ini rentan terhadap berbagai serangan, termasuk pencurian data, serangan man-in-the-middle, dan mengeksploitasi kelemahan kode. Banyak komponen program yang diekspor tanpa dienkripsi, sehingga memungkinkan aplikasi

pihak ketiga untuk mencuri data atau mengirimkan malware. Selain itu, banyak aplikasi yang meminta izin berbahaya yang dapat membahayakan privasi pengguna, seperti akses ke lokasi, kontak, dan pesan SMS. Penggunaan program yang disesuaikan, seperti GB WhatsApp, sangat dilarang karena menempatkan perangkat dan data pribadi pengguna dalam bahaya.

Gambar.8. Informasi File GB WhatsApp

MobSF menemukan banyak kelemahan utama dalam kode GB WhatsApp v31.15, yang dapat membahayakan privasi dan keamanan pengguna. Salah satu kelemahan utamanya adalah Konfigurasi Keamanan Jaringan, yang memungkinkan aplikasi berkomunikasi melalui lalu lintas teks biasa, sehingga rentan terhadap serangan man-in-the-middle (MitM). Selain itu, aplikasi ini ditemukan memiliki kerentanan Janus, yang memungkinkan file APK diperbarui tanpa membatalkan tanda tangan digital pada perangkat yang menjalankan Android 5.0 hingga 8.0. MobSF juga menemukan bahwa beberapa komponen aplikasi diekspor tanpa keamanan yang memadai, sehingga dapat diakses oleh pihak ketiga yang tidak berwenang.

Gambar.9. Hasil Pemindaian Tingkat Keparahan pada WhatsApp GB

Hasil Pemindaian Tingkat Keparahan pada GB WhatsAppGB WhatsApp juga mencari izin berbahaya lainnya, termasuk READ_PHONE_STATE untuk mengakses informasi perangkat, ACCESS_FINE_LOCATION untuk memantau posisi pengguna, dan READ_CONTACTS untuk membaca informasi kontak. Program ini bahkan dapat menerima SMS tanpa sepengetahuan pengguna dengan izin RECEIVE_SMS, dan memiliki akses penuh ke penyimpanan eksternal dengan MANAGE_EXTERNAL_STORAGE, yang memungkinkannya untuk mengubah data perangkat.

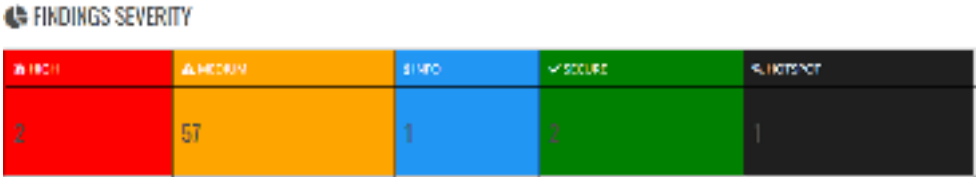
MobSF juga mengidentifikasi aktivitas yang mencurigakan, seperti potensi pengiriman SMS yang tidak sah, melacak posisi perangkat, mengakses informasi kontak, dan menutupi aktivitas berbahaya dengan menggunakan kode yang disamarkan. Strategi ini sering digunakan oleh malware untuk menghindari deteksi oleh solusi keamanan, sehingga meningkatkan kekhawatiran keamanan pengguna.

b. FM WhatsApp

Menurut hasil pemindaian dari Mobile Security Framework (MobSF), aplikasi WhatsApp FM memiliki skor keamanan 50/100, yang mengindikasikan tingkat risiko menengah. Program ini ditemukan memiliki beberapa kelemahan potensial yang dapat membahayakan keamanan perangkat dan privasi pengguna.

Gambar.10. Informasi File FM WhatsApp

Aplikasi ini menandatangani file APK menggunakan sertifikat digital asli, namun MobSF menemukan bahwa aplikasi ini masih rentan terhadap kerentanan Janus pada perangkat Android yang menjalankan versi 5.0 hingga 8.0. Bug ini memungkinkan APK yang telah ditandatangani untuk dimodifikasi tanpa mengubah tanda tangan digitalnya.



Gambar.11. Hasil Pemindaian Tingkat Keparahan pada FM WhatsApp

Hasil pemindaian MobSF menemukan bahwa aplikasi WhatsApp FM memiliki izin dan kerentanan yang berisiko tinggi. Menggunakan program ini dapat membahayakan keamanan perangkat dan privasi pengguna, terutama karena program ini dapat mengakses data pribadi, mengirim pesan tanpa sepengetahuan pengguna, dan terhubung ke jaringan yang tidak aman. Oleh karena itu, Anda disarankan untuk menghindari menginstal program khusus seperti FM WhatsApp dan sebagai gantinya gunakan aplikasi resmi yang tersedia di pasar yang dapat dipercaya seperti Google Play Store.

c. WhatsApp Plus

Temuan pemindaian MobSF mengungkapkan bahwa WhatsApp Plus v18.30 mengandung berbagai izin dan kerentanan berbahaya yang dapat membahayakan keamanan perangkat dan privasi pengguna. Skor keamanan yang hanya 49/100 menunjukkan bahwa perangkat lunak tersebut memiliki risiko sedang. Akibatnya, penggunaan aplikasi yang disesuaikan seperti WhatsApp Plus tidak dianjurkan karena dapat mengekspos kelemahan keamanan yang dapat dieksploitasi oleh pihak-pihak jahat.

Gambar.12. Informasi File of WhatsApp Plus

Temuan pemindaian MobSF mengungkapkan bahwa WhatsApp Plus v18.30 mengandung berbagai izin dan kerentanan berbahaya yang dapat membahayakan keamanan perangkat dan privasi pengguna. Skor keamanan yang hanya 49/100 menunjukkan bahwa perangkat lunak tersebut memiliki risiko sedang. Hasilnya, penggunaan MobSF menunjukkan bahwa aplikasi WhatsApp Plus v18.30 mencari berbagai hak akses berbahaya yang dapat membahayakan privasi dan keamanan pengguna. Hak-hak tersebut termasuk READ_PHONE_STATE, yang dapat digunakan untuk mencuri identitas pengguna, dan ACCESS_FINE_LOCATION, yang memungkinkan aplikasi untuk memantau keberadaan perangkat melalui GPS. Selain itu, aplikasi dapat mengakses data kontak pengguna melalui izin READ_CONTACTS dan menerima pesan SMS tanpa sepengetahuan pengguna dengan izin RECEIVE_SMS, serta mengelola penyimpanan eksternal melalui izin MANAGE_EXTERNAL_STORAGE, yang berpotensi mengarah pada manipulasi data pada perangkat.

Gambar.13. Hasil Pemindaian Tingkat Keparahan pada WhatsApp Plus

Selain kerentanan ini, aplikasi WhatsApp Plus v18.30 terlibat dalam berbagai tindakan meragukan yang dapat membahayakan keamanan perangkat pengguna. Program ini dapat mengirim pesan SMS tanpa izin pengguna, mengakses dan memantau lokasi perangkat, serta membaca dan menulis informasi kontak pengguna. Selain itu, program ini menggunakan kode yang disamarkan untuk menghindari deteksi oleh alat keamanan, yang merupakan metode umum yang digunakan oleh malware untuk menyembunyikan perilaku berbahaya.

V. Kesimpulan dan Saran

Berdasarkan analisis menggunakan VirusTotal dan Mobile Security Framework (MobSF), ditemukan bahwa aplikasi WhatsApp yang telah dimodifikasi seperti GB WhatsApp v31.15, FM WhatsApp v10.10, dan WhatsApp Plus v18.30 memiliki risiko keamanan data dan privasi pengguna yang cukup besar. Analisis VirusTotal menunjukkan bahwa aplikasi-aplikasi tersebut terdeteksi oleh berbagai vendor antivirus yang berpotensi mengandung malware, trojan, atau perangkat lunak berbahaya lainnya. Beberapa ancaman yang teridentifikasi termasuk pencurian data pribadi, akses tidak sah ke perangkat, dan pengiriman data ke server yang tidak dikenal. MobSF juga mengungkapkan bahwa aplikasi yang dimodifikasi ini memiliki skor keamanan yang rendah karena kerentanan kritis, seperti kerentanan Janus dan konfigurasi keamanan jaringan yang lemah, yang memungkinkan serangan seperti man-in-the-middle (MitM) dan manipulasi file APK.

Sebaliknya, aplikasi WhatsApp resmi menunjukkan tingkat keamanan yang jauh lebih tinggi, dengan tidak ada ancaman yang terdeteksi oleh 65 vendor keamanan. Fakta ini menegaskan bahwa penggunaan aplikasi yang dimodifikasi sangat berisiko bagi privasi dan keamanan pengguna. Aplikasi yang dimodifikasi diketahui meminta izin berbahaya, seperti akses ke lokasi perangkat, kontak, SMS, dan penyimpanan eksternal, yang dapat digunakan untuk aktivitas berbahaya, termasuk manipulasi data perangkat dan pengawasan yang tidak sah.

Gambar.14. Informasi File WhatsApp Versi Resmi

Disarankan bagi pengguna untuk tidak menggunakan aplikasi yang dimodifikasi seperti GB WhatsApp, FM WhatsApp, atau WhatsApp Plus karena risiko keamanan yang signifikan. Sebagai gantinya, gunakan aplikasi WhatsApp resmi yang diunduh melalui platform tepercaya seperti Google Play Store untuk meminimalkan risiko serangan malware dan pencurian data.

Untuk aplikasi yang dimodifikasi, para pengembang aplikasi disarankan untuk meningkatkan transparansi mengenai kebijakan privasi dan keamanan aplikasi. Selain itu, pengembang perlu memastikan kode aplikasi bebas dari kerentanan kritis yang dapat dieksploitasi oleh pihak-pihak yang tidak bertanggung jawab.

LAMPIRAN

Tabel.A1. Variabel Indikator Pertanyaan

Variabel	Indikator	Pertanyaan Penelitian
Risiko keamanan data dari mod whatsapp melalui pendekatan malware dan efeknya (X)	Frekuensi Penggunaan Aplikasi	1. Apakah anda pernah menggunakan Whatsapp Mod dan Menggunakannya setiap hari?
	Perhatian terhadap izin aplikasi	2. Saya memperhatikan izin aplikasi saat mengunduh whatsapp mod
	Kekhawatiran atas Penyadapan Data	3. Saya khawatir dengan potensi penyadapan data melalui whatsapp mod
	Kewaspadaan terhadap Risiko Malware	4. Saya menyadari risiko malware yang mungkin ada pada whatsapp mod
	Kepatuhan terhadap Pembaruan Aplikasi	5. Saya mengunduh versi terbaru whatsapp mod setiap kali ada pembaruan
	Motivasi untuk Menggunakan Whatsapp Mod	6. Apa alasan utama anda menggunakan whatsapp mod dibandingkan dengan whatsapp resmi
	Kendala Penggunaan	7. Apa saja kendala yang pernah anda alami dalam penggunaan whatsapp mod?
	Kepentingan Privasi	1. Saya merasa privasi sangat penting bagi saya dalam penggunaan whatsapp mod

Privasi Pengguna (Y)	Persepsi terhadap Regulasi	2. Menurut anda, seberapa penting regulasi atau perlindungan pengguna untuk aplikasi modifikasi seperti whatsapp mod?
	Perbandingan Keamanan	3. Bagaimana pendapat anda tentang keamanan whatsapp

VI. Referensi

[1] Oluwaseun Oladeji Olaniyi and Dagogo Sopriala Omubo, "WhatsApp Data Policy, Data Security and Users' Vulnerability," *International Journal of Innovative Research and Development*, May 2023, doi: 10.24940/ijird/2023/v12/i4/apr23021.

[2] A. Abadi Pamungkas and A. Susilo Yuda Irawan, "Analisis Penerapan Algoritma Kriptografi Rivest-Shamir-Adleman (RSA) dan Zero-Knowledge Proof Pada Aplikasi Whatsapp Mod," *Jurnal Ilmiah Wahana Pendidikan, Juli*, vol. 2023, no. 13, pp. 81–95, doi: 10.5281/zenodo.8145614.

[3] A. Whatsapp *et al.*, "Arus Jurnal Sosial dan Humaniora (AJSH)," vol. 4, no. 1, 2024, [Online]. Available: http://jurnal.ardenjaya.com/index.php/ajshhttp://jurnal.ardenjaya.com/index.php/ajsh

[4] B. Santoso, M. A. Ghofur, and J. Kuswanto, "Analysis of WhatsApp Mod User Awareness Information Security with Static Analysis Methods and Quantitative Methods," *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO)*, vol. 3, pp. 213–222, Dec. 2021, doi: 10.54706/senastindo.v3.2021.128.

[5] A. S. Shridhar Kakade and S. Khaiyum Professor, "Data Leaks and Its Prevention In Mobile Application." [Online]. Available: www.ijert.org

[6] R. Kuswulandari, A. Wirid, I. Jowanka, T. Nabila, P. Riyanto, and T. Listiani, "Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Aplikasi Whatsapp."

[7] T. Pangaribuan, Diana Sari, Caecilia Suprapti Dwi Takariani, and O. Simatupang, "KESADARAN KEAMANAN DAN PRIVASI DATA PENGGUNA WHATSAPP (STUDI KASUS DI PROVINSI JAWA BARAT)," *Jurnal Studi Komunikasi dan Media*, vol. 27, no. 1, pp. 93–108, Jun. 2023, doi: 10.17933/jskm.2023.5129.

[8] S. Yadav and N. Tiwari, "Privacy preserving data sharing method for social media platforms," *PLoS One*, vol. 18, no. 1 January, Jan. 2023, doi: 10.1371/journal.pone.0280182.

[9] I. Himawan *et al.*, "ANALISIS KEAMANAN INFORMASI MALWARE TERHADAP APLIKASI APK DENGAN METODE STATIC ANALYSIS MENGGUNAKAN MOBSF."

[10] M. R. Ramadhani and A. Raf'ie Pratama, "Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Indonesia."

[11] M. Zulfahmi, A. Elsandi, A. Apriliansyah, M. S. Anggreainy, K. Iskandar, and S. Karim, "Privacy protection strategies on social media," in *Procedia Computer Science*, Elsevier B.V., 2022, pp. 471–478. doi: 10.1016/j.procs.2022.12.159.

[12] S. Navaneethan and S. Udhaya Kumar, "ScanSavant: Malware Detection for Android Applications with Explainable AI," *International Journal of Interactive Mobile Technologies* , vol. 18, no. 19, pp. 171–181, Oct. 2024, doi: 10.3991/ijim.v18i19.49437.

[13] S. Abdelhay, A. M. A. Draz, W. A. K. Tharwat, and A. Marie, "The impact of using WhatsApp on the team's communication, employee performance and data confidentiality," *International Journal of Data and Network Science*, vol. 8, no. 2, pp. 1307–1318, Mar. 2024, doi: 10.5267/j.ijdns.2023.11.004.

[14] F. P. N. Koten, A. Jufriansah, and H. Hikmatiar, "Analisis Penggunaan Aplikasi Whatsapp sebagai Media Informasi dalam Pembelajaran: Literature Review," *Jurnal Ilmu Pendidikan (JIP) STKIP Kusuma Negara*, vol. 14, no. 1, pp. 72–84, Jul. 2022, doi: 10.37640/jip.v14i1.1409.

[15] A. Caleb, "Malware and Spyware in Mobile Applications." [Online]. Available: https://www.researchgate.net/publication/381582917