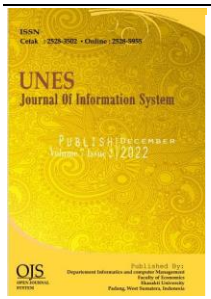


UNES Journal of Information System

Volume 8, Issue 1, June 2023

P-ISSN 2528-3502

E-ISSN 2528-5955

Open Access at: https://fe.ekasakti.org/index.php/UJIS

ANALISA KEAMANAN INFORMASI PENGGUNA INSTANDER DENGAN METODE ANALISIS DAN METODE KUANTITATIF

INSTANDER USER INFORMATION SECURITY ANALYSIS USING ANALYSIS METHOD AND QUANTITATIVE METHOD

Dedek Indra Gunawan Hts[1], Haris Asbari[2], Juli Ramadhani[3], Sinta Makito[4], Imam Syazali Lubis[5]

[1,2,3,4,5] Program Studi Informatika Fakultas Teknik dan Ilmu Komputer Universitas Potensi Utama.

E-mail : dedek.indra@gmail.com, asbari99@gmail.com, juliramadhani27@gmail.com, sintamakito@gmail.com, imamlubis9000@gmail.com

INFO ARTIKEL

Koresponden:

Dedek Indra Gunawan Hutasuhut

dede.indra@gmail.com

Kata kunci

Instagram, Instander, Keamanan, Informasi

Website:

https://fe.ekasakti.org/index.php/UJIS

Hal: 028 - 033

ABSTRAK

Semakin berkembangnya teknologi juga meningkatkan penggunaan teknologi di dunia, dan ini berdampak baik atau buruk bagi keamanan informasi yang ada di dunia maya, keamanan informasi yang ada dapat menyebar melalui eksploitasi keamanan informasi dan berada di tangan. dari tidak bertanggung jawab rakyat lubang di setiap media informasi di dunia maya. Salah satu celah yang memungkinkan kejahatan menggunakan aplikasi tidak resmi, di mana aplikasi ini menawarkan fitur yang lebih menarik yang membuat pengguna menggunakan aplikasi tersebut. Diantara aplikasi yang banyak digunakan adalah chat jejaring sosial, yang dalam hal ini mengangkat isu pengguna Instander, dimana Instander menyediakan beberapa fungsi yang tidak terdapat pada aplikasi Instagram resmi di platform android. Ini bisa menjadi salah satu celah di mana pengembangan aplikasi tidak dilakukan secara resmi, di mana keamanan data dan informasi yang disebar luaskan melalui alat komunikasi Instander tidak dapat dijamin. Oleh karena itu, penelitian ini sebaiknya memberikan nilai persentase terkait tingkat kewaspadaan pengguna Instagram yang dapat digunakan sebagai kajian keamanan yang ada, dengan memperhatikan hasil analisis statis terkait celah keamanan Instander.

ARTICLE INFO

Corresponden:
Dedek Indra Gunawan Hutasuhut
dede.indra@gmail.com

Keywords:
Instagram, Instander, Information, Security

Website:
https://fe.ekasakti.org/index.php/UJIS

Page: 028 - 033

ABSTRACT

The development of technology also increases the use of technology in the world, and this has a good or bad impact on the security of information in cyberspace, existing information security can spread through information security exploitation and is in the hands. from the people's irresponsibility holes in every information media in cyberspace. One of the loopholes that allow crime to use unofficial applications, is where this application offers more interesting features that make users use the application. Among the applications that are widely used are chat social networks, which in this case raises the issue of Instander users, where Instander provides several functions that are not available in the official Instagram application on the Android platform. This can be one of the loopholes where application development is not carried out officially, where the security of data and information that is disseminated through Instander communication tools cannot be guaranteed. Therefore, this research should provide a percentage value related to the level of alertness of Instagram users that can be used as an assessment of existing security, taking into account the results of the static analysis regarding Instander's security loopholes.

PENDAHULUAN

Kini komunikasi instan menunjukkan perkembangan yang sangat pesat, seiring berjalannya waktu komunikasi instan menjadi sesuatu yang sangat dibutuhkan oleh para netizen di dunia, salah satu komunikasi instan yang paling populer adalah Instagram yang banyak digunakan saat ini. Berkat fitur yang sangat mudah digunakan seperti group chat, video call, pengiriman foto ke file dan juga ke ponsel yang tidak menggunakan pulsa, menjadikannya layanan pesan instan yang sangat populer di kalangan masyarakat segala usia.

Instagram memiliki efek positif, yaitu komunikasi bukan lagi jarak bukan lagi halangan, di balik efek positif Instagram juga memiliki efek negatif jika disalahgunakan, misalnya. Kejahatan atau perdagangan barang ilegal. Instander umumnya adalah Instagram, namun yang membedakannya dengan Instagram pada umumnya adalah fitur-fiturnya, beberapa orang memodifikasi atau menambahkan fitur yang tidak ada di Instagram resmi, Instander sendiri memiliki arti Intagram Mod yang menggunakan apk tambahan. Untuk mengambil data pengguna dan memperumit perangkat, individu tersebut dapat menggunakan perangkat untuk mendapatkan akses dan informasi pengguna untuk keuntungan pribadi dan merugikan pengguna dengan informasi pribadi .

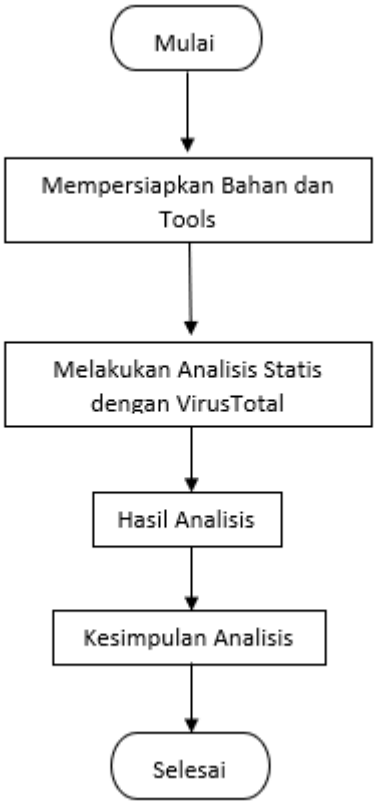
Hal ini dapat digunakan untuk merumuskan permasalahan yang dikaji untuk mendapatkan persentase tingkat kewaspadaan pengguna Instander terkait keamanan smartphone, dimana pemasangan aplikasi tidak resmi dapat

mengakibatkan kebocoran data yang dapat merugikan pengguna Instagram. Tujuan artikel ini adalah untuk mendapatkan nilai persentase dari survey tingkat kewaspadaan pengguna Instander guna menambah pengetahuan tentang kebocoran data yang disebabkan oleh program yang dimodifikasi atau ilegal.

METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini menggunakan penelitian dengan menggunakan metode kuantitatif. Metode kuantitatif adalah jenis metode penelitian yang sistematis, terencana dan terstruktur dengan jelas dari awal hingga akhir penelitian. Metode kuantitatif adalah "dalam filosofi positivisme, suatu metode mendasar dimana suatu populasi atau sampel tertentu dipelajari, alat penelitian juga digunakan untuk pengumpulan data, analisis data bersifat statistik/kuantitatif, tujuannya adalah untuk menguji hipotesis yang telah ditentukan sebelumnya.

Gambar 1. Diagram Proses analisis statis

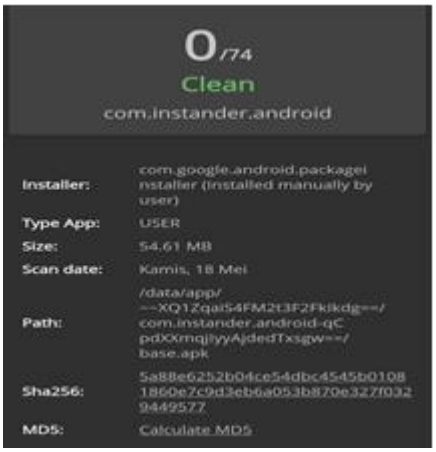


Langkah pertama analisis statis adalah menyiapkan alat analisis statis dan aplikasi Instagram Mod yaitu Instander. Langkah selanjutnya adalah melakukan analisis statis pada VirusTotal untuk mendapatkan hasil analisis. Disajikan dalam bentuk laporan yang ringkas dan mudah dipahami.

HASIL DAN PEMBAHASAN

Hasil Analisis Statis Menggunakan Virus Total

Gambar 2. Aplikasi Instander



Gambar 3. Hasil pengujian aplikasi Instander di Virus Total

Pada Instander, saat dilakukan analisis stastis dengan VirusTotal, VirusTotal mendeteksi 4 dari 46 mesin vendor antivirus adanya ancaman yang berada pada aplikasi tersebut, dan juga pada aplikasi ini VirusTotal mendeteksi adanya relasi terindikasi Malware. Pada Tabel 1 daftar deteksi yang terdeteksi diawal hasil analisis.

Tabel 1. Hasil Analisis Instander

Vendor	Deteksi	Keterangan
Avira	ANDROID/Dialer.FHJZ.Gen	virus yang mencoba membuat koneksi telepon dengan tarif tinggi secara signifikan.
Qihoo-360	Trojan.Android.Gen	aplikasi yang disisipkan ke dalam aplikasi
Tencent	A.Gray.VenomBanshee	keluarga dari virus A.Gray sebagai Adware
Trustlook	Android.PUA.DebugKey	aplikasi tersembunyi, yang tanpa sadar terunduh

Hasil Analisis

Persentase variabel A Data yang diperoleh dari variabel A pada penggunaan aplikasi Instander terlebih dahulu dicari nilai kriteria masing-masing variabel dengan menggunakan rumus:

∑SK = Skor tertinggi tiap pertanyaan x jumlah item pertanyaan x jumlah responden yang ada.

∑SK = 5 x 2 x 50

∑SK = 500

Dengan demikian nilai SK variabel A adalah 500, setelah didapatkan nilai tersebut dilakukan perhitungan untuk menjumlahkan nilai respon dari variabel A.

	Pertanyaan		
	1	2	Total
Total	192	197	389
Persentase	49,4%	50,6%	100%

Gambar 4. Skor Jawaban Variabel A

Berdasarkan angka skor untuk pertanyaan variabel A tentang pemahaman cara menggunakan Instander, dilakukan perhitungan untuk mendapatkan nilai persentase dengan menggunakan rumus:

Persentase Variabel A = Total skor yang didapat SK x 100 = 389500 x 100 = 77,8%

Berdasarkan hasil perhitungan, persentase pemahaman pengguna Instander adalah 77,8%.

SIMPULAN

Pada variabel A dengan topik pembahasan tingkat pemahaman pengguna Instander tentang dasar penggunaan Instander mendapatkan persentase sebesar 77,8% yang menandakan bahwa pengguna Instander termasuk dalam kategori paham tentang risiko penggunaan Instander dalam kegiatan sehari-hari. Cukup sadar dalam mengamankan dan memperhatikan smartphone pribadinya. Pada hasil Analisis menggunakan VirusTotal mendeteksi bahwa Instander yang digunakan sebagai bahan pendukung penelitian ini terdapat setidaknya dua ancaman yang dapat merugikan pengguna dan perangkat yang digunakan. Pada hasil Analisis menggunakan VirusTotal ada Tabel Perijinan ketiga aplikasi banyak mendapatkan status Berbahaya atau Dangerous pada perijinan yang ada pada aplikasi sedangkan pada tabel analisis kode didapatkan hasil isu yang menjadi kerentanan aplikasi Instander tersebut tidak sesuai dengan Standar yang ada.

UCAPAN TERIMAKASIH

Terimakasih kepada seluruh penulis yang sudah berpatisipasi dalam membangun artikel ilmiah ini.

DAFTAR PUSTAKA

N. Anwar and I. Riadi, "Analisis Investigasi Forensik Instander Smartphone Terhadap Instagram Berbasis Web," J. Ilm. Tek. Elektro Komput. dan Inform., vol. 3, no. 1, p. 1, 2017, doi: 10.26555/jiteki.v3i1.6643.

G. M. Zamroni, R. Umar, and I. Riadi, "Analisis Forensik Aplikasi Instant Messaging Berbasis Android," vol. 2, no. 1, pp. 102–105, 2016, [Online]. Available: http://ars.ilkom.unsri.ac.id.

C. Hanifurohman and D. D. Hutagalung, "Analisis Statis Menggunakan Mobile Security Framework Untuk Pengujian Keamanan Aplikasi Mobile E-

Commerce Berbasis Android," Sebatik, vol. 24, no. 1, pp. 22–28, 2020, doi: 10.46984/sebatik.v24i1.920.

Sugiyono, "Metode Penelitian Manajemen. ALFABETA. Bandung," ALFABETA, 2014.

Sugiyono, "Prof. Dr. Sugiyono. 2018. Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Bandung: Alfabeta.," Prof. Dr. Sugiyono. 2018. Metod. Penelit. Kuantitatif, Kualitatif, dan R&D. Bandung Alf., 2018. [8] D. N. J. Arum and Anie, S t a t i s t i k d e s k r i p t i f & r e g r e s i l i n i e r b e r g a n d a d e n g a n s p s s. 2012.

IBM, "Statistik SPSS - Gambaran Umum | IBM." https://www.ibm.com/products/spss-statistics (accessed Jan. 08, 2021).

S. Zein, L. Yasyifa, R. Ghozi, E. Harahap, F. Badruzzaman, and D. Darmawan, "Pengolahan dan Analisis Data Kuantitatif Menggunakan Aplikasi SPSS," J. Teknol. Pendidik. dan Pembelajaran, vol. 4, no. 1, pp. 1–7, 2019.

T. A. Cahyanto, V. Wahanggara, and D. Ramadana, "Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis," Justindo, J. Sist. Teknol. Inf. Indones., vol. 2, no. 1, pp. 19– 30, 2017, [Online]. Available: http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO/article/view/1037.

R. Adenansi and L. A. Novarina, "Malware dynamic," J. Educ. Inf. Commun. Technol., vol. 1, no. 1, pp. 37–43, 2017.

L. Song, H. Huang, W. Zhou, W. Wu, and Y. Zhang, "Learning from big malware," Proc. 7th ACM SIGOPS Asia-Pacific Work. Syst. APSys 2016, 2016, doi: 10.1145/2967360.2967367.

R. Masri and M. Aldwairi, "Automated malicious advertisement detection using VirusTotal, URLVoid, and TrendMicro," 2017 8th Int. Conf. Inf. Commun. Syst. ICICS 2017, pp. 336–341, 2017, doi: 10.1109/IACS.2017.7921994.

Weriza, J., Malisza, D., Dahri, N., & Susanti, M. (2021). RESTAURANT MENU DESIGN MUARO NEW SAND JAMAK. Dinasti International Journal of Digital Business Management, 2(6), 1063-1069.

Siregar, J. J. (2013). Analisis explotasi keamanan web denial of service attack. ComTech: Computer, Mathematics and Engineering Applications, 4(2), 1199-1205.