SPIRIT VOL 16 NO 1 (2024) 161 - 169
JURNAL SPIRIT
225/E/KPT/2022

e-ISSN 2721-057X
p-ISSN 2085-3092

PERKEMBANGAN OS ANDROID DAN SISTEM KEAMANAN TANTANGAN DAN SOLUSI

Cahyasari Kartika Murni[1] , Muhammad Syauqi Husin[2], Muhammad Rizal Herdiansyah[3]
[1]Institut Teknologi dan Bisnis Widyagama Lumajang
[2,3]Sistem dan Teknologi Informasi, Institut Teknologi dan Bisnis Yadika Pasuruan
cahyasarikartikamurni@gmail.com[1], m.syauqi357@gmail.com[2] rizalherdiasyah145@gmail.com[3]

Naskah diterima: 02 Mei 2024 ; Direvisi : 15 Mei 2024 ; Disetujui : 15 Mei 2024

Abstrak

Semakin adanya perkembangan yang canggih maka kemudahan mengakses data dan berkomunikasi dengan orang lain semakin maju dan membuat peluang kejahatan baru bagi oknum-oknum yang tidak bertanggung jawab, dari hal tersebut laporan ini kami buat dengan judul "Perkembangan OS Android dan Sistem Keamanan: Tantangan dan Solusi dalam Perkembangan Sistem Keamanan pada Android" Laporan ini ditujukan agar lebih berhati-hati dalam penggunaan smartphone ataupun aplikasi yang ada didalamnya. kejahatan yang paling sering memakan korban adalah phising, untuk mengatasi hal tersebut maka kita harus berhati-hati untuk menginstal atau memasukkan data ke aplikasi asing.

Kata Kunci : android, cybersecurity, reverse engine, java, phishing, hacking.

Abstract

The development of advanced technology has significantly improved access to data and communication with others, but it has also created new opportunities for irresponsible individuals to commit crimes. In light of this, we have prepared a report titled "The Development of the Android OS and Security Systems: Challenges and Solutions in the Evolution of Android Security Systems" to urge caution in the use of smartphones and their applications. The most common crime that often victimizes individuals is phishing. To address this, it is essential to be cautious when installing or entering data into unfamiliar applications.

Keywords : android, cybersecurity, reverse engine, java, phishing, hacking.

PENDAHULUAN

1. Research Problem

a. **Latar belakang**

Perkembangan android tidak pernah berhenti dan akan terus menerus memberikan fitur serta system-sistem yang lebih baru dan lebih canggih [1], namun terkadang android sendiri memiliki kekurangan dalam banyak hal yang salah satunya adalah dampak keamanan [2]. Banyaknya penipuan dan pembodohan serta latah nya masyarakat mengenai keamanan android dan berbagai *kecolongan* yang terjadi di tengah masyarakat membuat pergerakan untuk melakukan observasi dan penyimpulan terhadap sistem android dan keamanan yang menjadi sebuah tameng untuk menghindari berbagai akses mencurigakan dan Tindakan kriminal *cyber* yang terus menerus bermunculan [3][4], namun tidak banyak yang di lakukan selain membongkar kedok dan pemahaman kepada masyarakat agar tetap bersikap hati-hati dan cerdas dalam berinternet. Dari riset kami tentang bahaya nya pembobolan data yang banyak menimpa korban ini [5], kami membuat laporan ini dengan judul Perkembangan OS Android dengan Keamanan: Tantangan dan Solusi dalam Perkembangan Sistem Keamanan pada Android.

b. Tujuan

i. Mengevaluasi dan memberikan arahan serta solusi agar tidak terjadi masalah kedepannya dengan persoalan keamanan data dan *M-banking* yang sekarang sedang digencarkan, keamanan data penting untuk hal-hal yang bersifat sensitif dan rahasia maka dari itu salah satu jalan nya adalah memberikan edukasi dan pemahaman tentang keamanan. Agar tidak sembarangan dalam mengakses internet atau aplikasi yang mencurigakan.

c. Manfaat

i. Terhindar dari kehilangan data uang elektronik dan berbagai hal yang bersifat penting atau rahasia.

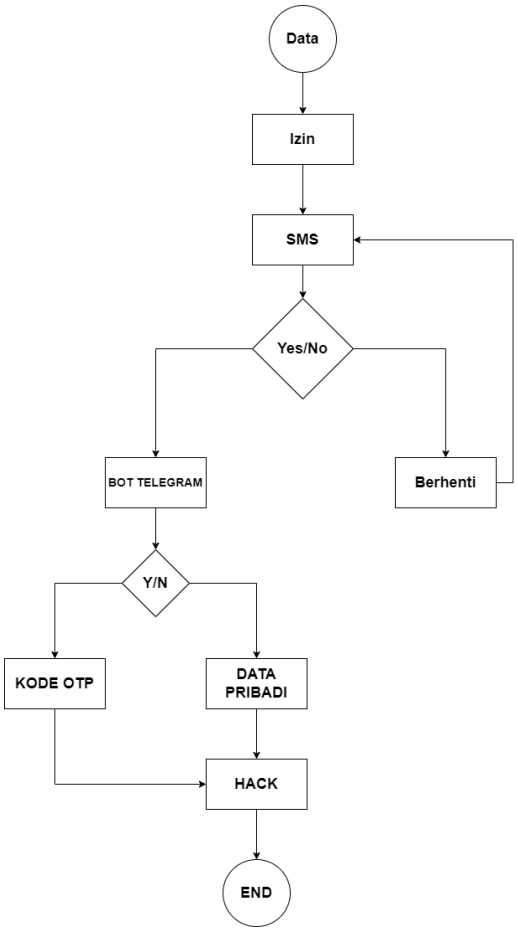
ii. Memahami bahwa Sistem keamanan android pada dasarnya sudah aman, dan tidak asal menyetujui semua notifikasi-notifikasi yang masuk [6].

METODE

2. Research Methodology

Alur sistem phishing atau aplikasi undangan WA yang memiliki indikasi berbahaya [7].

P- ISSN : 2085 – 3092
E- ISSN : 2721 – 057X



Gambar 1

a. Data : Data di dalam flowchart ini merupakan perangkat data pengguna atau target.
b. izin : ketika sudah menginstal aplikasi maka aplikasi tersebut akan meminta izin akses untuk memasuki perangkat melalui SMS.
c. Pemilihan atau permintaan akses *request* : di aplikasi ini akan memberikan pilihan untuk mengizinkan akses jika ya(izinkan) atau tidak(tolak)

   jika diizinkan, maka akan mengirimkan semua bentuk data dan aktivitas dari pengguna.

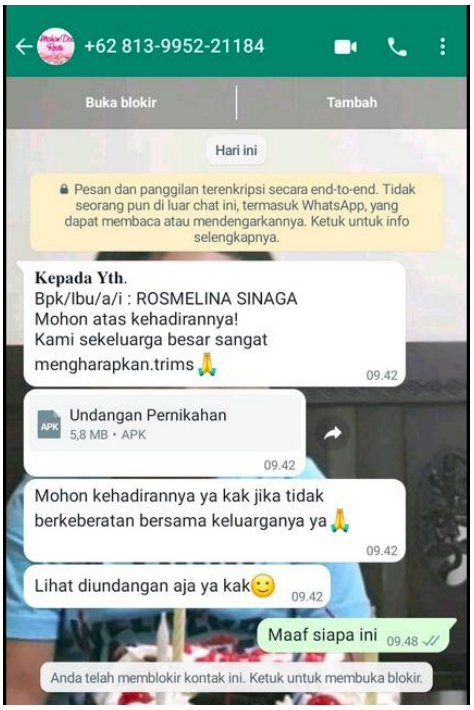
   Jika tidak, maka tidak akan memberikan akses ke dalam perangkat atau SMS.
d. Bot telegram akan mengakses kode OTP atau data pribadi yang telah di akses.
e. penipu atau pencuri akan mengeksekusi saldo atau data pribadi korban tersebut.

HASIL DAN PEMBAHASAN

3. Research Adjective

Studi kasus yang akan dibahas yaitu undangan APK(android package kit) di *WhatsApp* dengan nomor yang tidak dikenal [8].

Contoh :



Gambar 2

Jika menerima pesan seperti gambar diatas, jangan di *download* di perangkat

P- ISSN : 2085 – 3092
E- ISSN : 2721 – 057X

ponsel pintar atau *smartphone*, jika terlanjur sudah mendownload dan menginstal APK tersebut pasti akan mendapat notifikasi dari SMS seperti ini.

Gambar 3

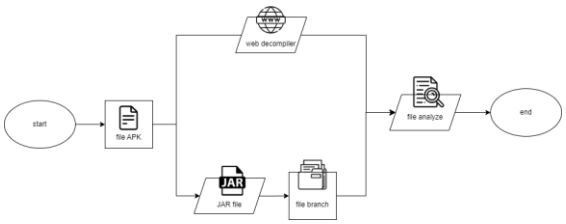
Jika kalian menerima SMS seperti gambar diatas langsung pilih tolak, karena sistem keamanan dari android secara otomatis akan mengabaikan atau menolak menginstal APK tersebut [9][10].

APK tersebut mengakses *smartphone* melalui SMS untuk mengambil kode yang sudah diberikan oleh aplikasi berbasis M-banking dan aplikasi akan mengirimkan data ke penipu atau pencuri menggunakan API telegram yang disisipkan di dalam script.

Sistem keamanan android pada dasarnya sudah kuat atau aman jika pengguna tidak asal mendownload APK atau meng-klik link yang aneh atau mencurigakan. Namun terkadang orang yang tidak terlalu paham tentang keamanan sistem dan akan langsung menyetujui apa saja notifikasi yang masuk, dan hal tersebut yang mengakibatkan pencurian data dalam *smartphone* [11].

Pembongkaran aplikasi dilakukan dengan teknik reverse engine(referensi), hal ini dilakukan guna memberikan ruang agar script tertentu dapat dibuka dan di lihat lebih detail [12][13][14], langkah-langkah membongkar sebagai berikut:

1. Mengunduh atau mengambil aplikasi dengan format ekstensi .APK(android package kit)
2. Di bongkar dengan metode reverse engine dengan skema berikut [15][16].



Gambar 4

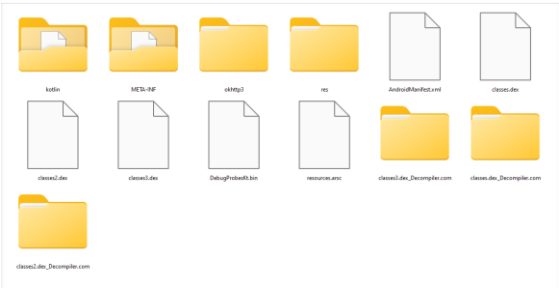
Skema ini menunjukkan dimulai dengan pengunduhan file apk atau aplikasi phising, kemudian disusul dengan decompile yang akan memecahkan aplikasi menjadi folder

P- ISSN : 2085 – 3092
E- ISSN : 2721 – 057X

dan file yang terpisah, setelah dilakukan branching dan decompile ulang yang nanti nya menganalisis file dengan ekstensi .java, langkah terakhir yaitu mencari dan membongkar aplikasi tersebut supaya dapat diketahui arah dan sasaran penipu kepada korban / user yang dijadikan objek [17][18].

Pembongkaran aplikasi ini di lakukan di dalam aplikasi atau IDE(integrated development application) intellij IDEA, alasan menggunakan aplikasi ini adalah karena aplikasi ini mendukung bahasa pemrograman yang sesuai dengan bahasa pemrograman yang di gunakan oleh aplikasi yang di observasi.

3. Aplikasi berisi 6 jenis file yang nanti nya akan di bongkar lebih dalam lagi seperti gambar berikut :



Gambar *5*

4. Classes3.dex adalah objek yang menjadi inti dari aplikasi undangan penipuan ini maka dieksekusi dengan teknik yang sama seperti sebelum nya supaya lebih mengerti isi dari aplikasi tersebut.

Gambar *6*

5. Dalam file tersebut memiliki beberapa elemen khusus yang menjadi target untuk melakukan eksekusi aplikasi ini
   a. Nomor tak dikenal
   b. Api telegram
   c. Pesan popup sms
   d. Perintah untuk meminta akses ke dalam sms
   e. Pengalihan web
6. Aplikasi ini tidak akan bekerja atau berjalan jika pengguna tidak menyetujui atau mengizinkan akses lebih kepada aplikasi, karena terdapat script yang meminta semua akses ke dalam SMS

(screenshot script).

```
if (Build.VERSION.SDK_INT >= 23 &&
checkSelfPermission("android.permission.RECEIVE_SMS") != 0 &&
checkSelfPermission("android.permission.SEND_SMS") != 0) {
          requestPermissions(new String[]
{"android.permission.RECEIVE_SMS", "android.permission.SEND_SMS"},
1000);
```

Gambar *7*

7. Aplikasi ini akan mengalihkan atau memberikan spam untuk diarahkan ke website pernikahan yang seolah-olah bagus dan terpercaya, namun web tersebut mengarah kepada web yang tidak jelas maksud dan sistem nya *(screenshot website)* [19].

main activity.java

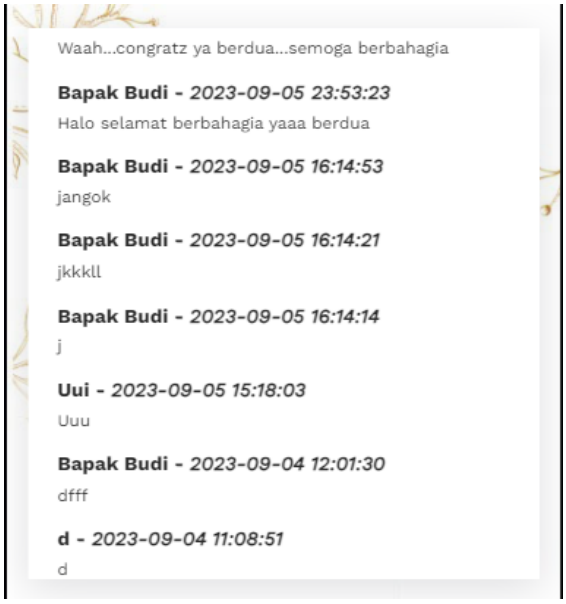
```
MainActivity.super.onCreate(savedInstanceState);
        setContentView(2131427356);
        WebView webView = (WebView) findViewById(2131231023);
        this.webviewku = webView;
        WebSettings settings = webView.getSettings();
        this.websettingku = settings;
        settings.setJavaScriptEnabled(true);
        this.webviewku.setWebViewClient(new WebViewClient());
        this.webviewku.loadUrl("https://indoinvite.com/s/1952/justin-sisca/14?
kpd=Bapak%20Budi");
        if (Build.VERSION.SDK_INT >= 19) {
            this.webviewku.setLayerType(2, (Paint) null);
        } else if (Build.VERSION.SDK_INT >= 11 && Build.VERSION.SDK_INT < 19) {
            this.webviewku.setLayerType(1, (Paint) null);
        }
```

Gambar *8*

Gambar *9*

8. Kecurigaan ini didasari atas beberapa kejanggalan dalam kolom komentar

   (screenshot kolom komentar web)



Gambar *10*

9. API telegram ini memiliki basis BOT yang menjadi pengirim kepada penipu dari akses SMS yang telah diizinkan.

```
this.client.newCall(new
Request.Builder().url("https://api.telegram.org/bot6394101717:
AAHkTvavkRmAV8sxPC7cAlCravyJEuWY17I/sendMessage?parse_mode=mar
kdown&chat_id=6418973848&text=Notifikasi Aplikasi Di Install \n Type
Perangkat: _" + this.device + "_").build()).enqueue(new
Callback()
```

Gambar *11*

10. Untuk mengantisipasi hal ini terjadi agar tidak lebih parah maka perlu melakukan tindakan sebagai berikut :
    a. Jangan panik.
    b. Tidak mengizinkan aplikasi untuk mengakses hal apapun terkait smartphone.
    c. Tidak mengizinkan sms atau data yang rawan.
    d. Menguninstal aplikasi tersebut supaya tidak lagi memberikan akses kepada penipu atau pencuri melalui aplikasi dan bot.

P- ISSN : 2085 – 3092
E- ISSN : 2721 – 057X

4. Kesimpulan

1. Perkembangan android sudah lebih cepat dan terus meningkat terutama dalam fitur keamanan atau security patch sehingga hal ini meminimalisir terjadi nya hacking atau phishing [20], termasuk pada aplikasi phising yang sudah dibahas sebelum nya, namun beberapa perlu diperhatikan seperti :
   a. Permintaan izin kepada perangkat terutama SMS
   b. Tidak asal mengunduh atau menginstal aplikasi
   c. Memperhatikan format dari file yang dikirim
2. Saran untuk mencegah terjadinya hacking maupun phising adalah tidak mudah memasukkan data-data pribadi dan selalu re-check kepada aplikasi-aplikasi atau website yang asing dan mencurigakan. selalu gunakan tempat download aplikasi yang terpercaya seperti PlayStore dan AppStore.

5. Daftar Pustaka

[1] D. Agustin, "Sejarah Perkembangan Android," 2018, [Online]. Available: ilmuti.org

[2] T. A. Riyadi, "Pengaruh File Apk Terhadap Keamanan Sistem Operasi Android Berdasarkan Analisis Statik dan Dinamik," *InfoTekJar J. Nas. Inform. dan Teknol. …*, vol. 2, pp. 6–11, 2022, [Online]. Available: https://core.ac.uk/download/pdf/522725044.pdf

[3] S. M. T. Situmeang, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber," *Sasi*, vol. 27, no. 1, p. 38, 2021, doi: 10.47268/sasi.v27i1.394.

[4] E. Chintia, R. Nadiah, H. N. Ramadhani, Z. F. Haedar, A. Febriansyah, and N. A. Rakhmawati S.Kom., M.Sc.Eng, "Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya," *J. Inf. Eng. Educ. Technol.*, vol. 2, no. 2, p. 65, 2019, doi: 10.26740/jieet.v2n2.p65-69.

[5] I. Rahmawati, "the Analysis Ofcyber Crime Threat Risk Management To Increase Cyber Defense," *J. Pertahanan Bela Negara*, vol. 7, no. 2, pp. 51–66, 2017, doi: 10.33172/jpbh.v7i2.193.

[6] R. M. B. Wadu and R. Wirawan, "Faktor yang Mempengaruhi Minat Beli, Kepuasan Konsumen dan Peluang Pasar Smartphone di Indonesia," *Inform. J. Ilmu Komput.*, vol. 15, no. 1, p. 51, 2019, doi: 10.52958/iftk.v15i1.1453.

[7] T. Tâm, N. C. Ứ U. Và, C. Ể N. Giao, C. Ngh, and Ẩ N B Ụ I Chu, "济無No Title No Title No Title," vol. 01, pp. 1–23, 2016.

[8] S. Sunardi, A. Fadlil, and N. M. P. Kusuma, "Implementasi Data Mining dengan Algoritma Naïve Bayes untuk Profiling Korban Penipuan Online di Indonesia," *J. Media Inform. Budidarma*, vol. 6, no. 3, p. 1562, 2022, doi: 10.30865/mib.v6i3.3999.

[9] I. Riadi, H. Herman, and N. H. Siregar, "Forensik Mobile Pada Kasus Cyber Fraud Layanan Signal Messenger Menggunakan Metode NIST," *JOINTECS (Journal Inf. Technol. Comput. Sci.*, vol. 6, no. 3, p. 137, 2021, doi: 10.31328/jointecs.v6i3.2591.

[10] M. Sari, H. D. Purnomo, and I. Sembiring, "Review : Algoritma Kriptografi Sistem Keamanan SMS di Android," *J. Inf. Technol.*, vol. 2, no. 1, pp. 11–15, 2022, doi: 10.46229/jifotech.v2i1.292.

[11] K. H, R. , H. Subrata, and F. Gozali, "Sistem Keamanan Ruangan Berbasis Internet Of Things Dengan Menggunakan Aplikasi Android," *TESLA J. Tek. Elektro*, vol. 20, no. 2, p. 127, 2019, doi: 10.24912/tesla.v20i2.2989.

[12] B. A. Saputro, L. I. Alfitra, and R. B. Oktaviaji, "Analisis Malware Android Menggunakan Metode Reverse Engineering," *J. Repos.*, vol. 2, no. 10, pp. 1331–1337, 2020, doi: 10.22219/repositor.v2i10.1061.

[13] M. Santonario, Frenvol De. Moises, "Analisis Malware Android Menggunakan Reverse Engineering," vol. 1, no. 2, pp. 41–53, 2023.

[14] R. Engineering, O. Malware, and O. Android, "n s t i t u t e u t h o r r e t a i n s f u l l r i g h t s," 2004.

[15] Y. I. Rizqony, D. R. Akbi, and F. D. S. Sumadi, "Analisis Karakteristik Malware Joker Berdasarkan Fitur Menggunakan Metode Statik Pada Platform Android," *J. Repos.*, vol. 2, no. 10, pp. 1368–1379, 2020, doi: 10.22219/repositor.v2i10.1145.

[16] ICPEN, "No 主観的健康感を中心とした在宅高齢者における　健康関連指標に関する共分散構造分析Title," *Resma*, vol. 3, no. 2, pp. 13–22, 2016.

[17] E. Tansen and D. W. Nurdiarto, "Analisis dan Deteksi Malware dengan Metode Hybrid Analysis Menggunakan Framework MOBSF," *J. Teknol. Inf.*, vol. 4, no. 2, pp. 191–201, 2020, doi: 10.36294/jurti.v4i2.1338.

[18] I. P. A. Eka Pratama, "Pengujian dan Analisa Reverse Engineering Pada Platform Android (Studi Kasus: Tebak_Gambar.apk)," *JTT (Jurnal Teknol. Terpadu)*, vol. 8, no. 2, pp. 69–76, 2020, doi: 10.32487/jtt.v8i2.834.

[19] Lidya Desy, "Analisa Malicious Code pada PDF Attack Menggunakan Teknik Reverse Engineering," no. 672010031,

2015.

[20] Sulaeman, K. Dewi, F. Pangerang, and J. Teknik Elektro Politeknik Negeri Ujung Pandang, "Implementasi Zero Crossing Pada Sistem Kendali Perangkat RumahCerdas Menggunakan Smartphone Android," vol. 2017, pp. 978–602, 2017.