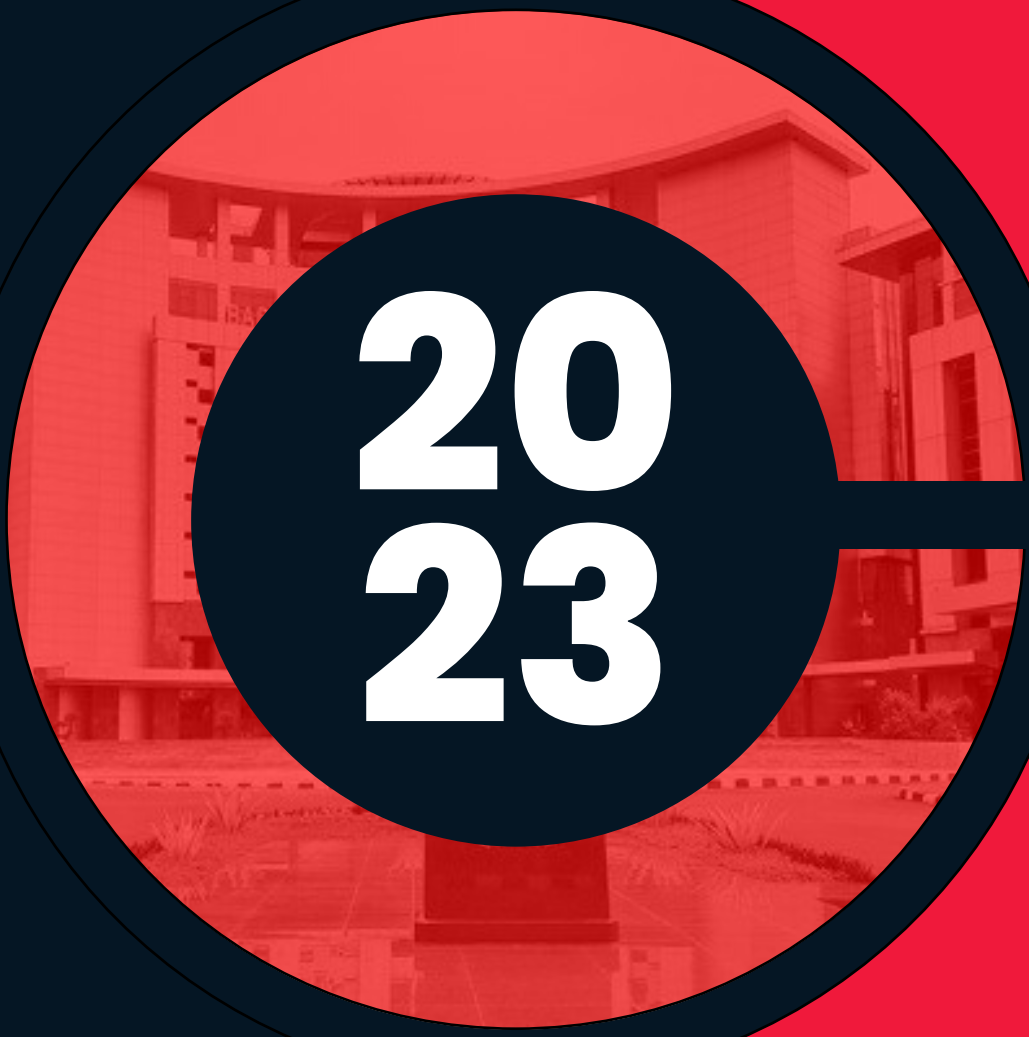
BADAN SIBER DAN SANDI NEGARA

TLP: Clear

# IMBAUAN KEAMANAN



# 2023

Penipuan dengan Modus Berkas Aplikasi Berbasis Android (.apk) melalui Surat Undangan Pernikahan

**28 Januari 2023**

# DAFTAR ISI

## Pendahuluan

- Terdapat temuan modus penipuan menggunakan berkas Android Package Kit (.apk) yang mengatasnamakan Surat Undangan Pernikahan
- Modus penipuan ini dapat mengakibatkan penyerang mendapatkan akses terhadap SMS korban dan dapat membuat token SMS-banking.

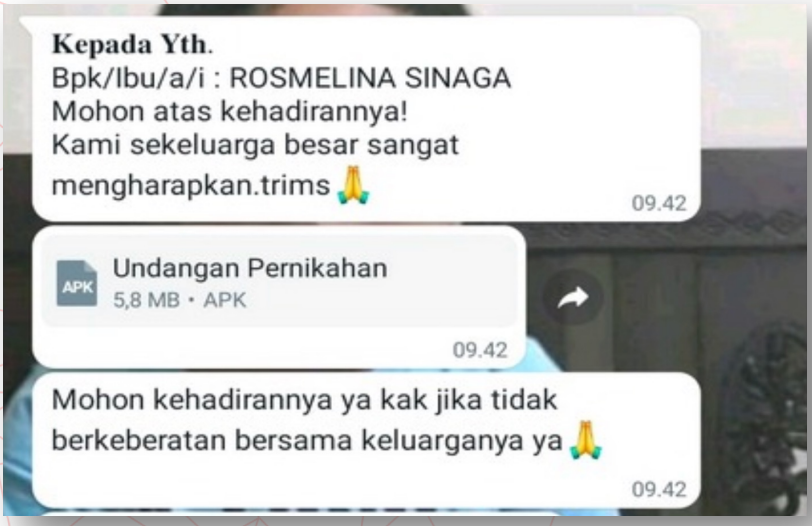

## Objek Terdampak

Obyek yang terdampak kerentanan ini adalah platform media social dari pengguna smartphone berbasis android

## Penjelasan

Android Package Kit (.apk) adalah format berkas yang digunakan untuk pemasangan perangkat lunak aplikasi pada perangkat berbasis Google Android.

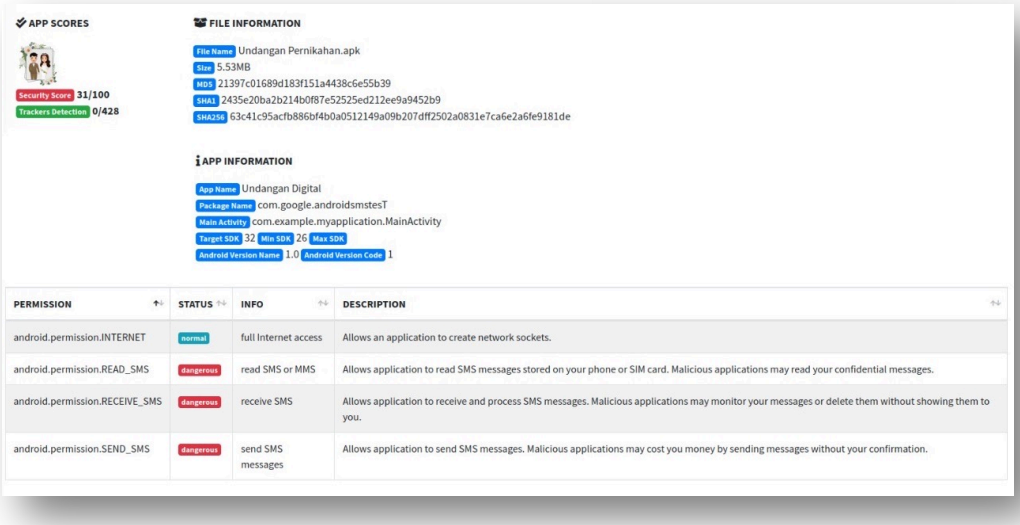
Terdapat modus penipuan dengan berkedok undangan pernikahan yang dikirimkan melalui media komunikasi Whatsapp. Penipu melakukannya dengan mengirimkan teks undangan dan diikuti dengan berkas .apk



# Penjelasan

Aplikasi tersebut dapat meminta akses untuk melakukan aktivitas sebagai berikut

- **Baca SMS atau MMS**. Jika diizinkan, aplikasi membaca pesan SMS yang tersimpan di HP atau kartu SIM. Aplikasi ini memungkinkan untuk membaca pesan rahasia milik korban.
- **Terima SMS**. Jika diizinkan, aplikasi menerima dan memproses pesan SMS. Aplikasi ini memungkinkan untuk melakukan monitor atau menghapus pesan tanpa memperlihatkannya kepada korban.
- **Kirim SMS**. Jika diizinkan, aplikasi mampu mengirimkan pesan SMS. Aplikasi ini memungkinkan untuk dikenai biaya saat mengirimkan pesan tanpa konfirmasi kepada korban.



APP SCORES

Security Score 31/100
Trackers Detection 0/428

FILE INFORMATION

File Name Undangan Pernikahan.apk
Size 5.53MB
MD5 21397c01689d183f151a4438c6e55b39
SHA1 2435e20ba2b214b0f87e52525ed212ee9a9452b9
SHA256 63c41c95acfb886bf4b0a0512149a09b207dff2502a0831e7ca6e2a6fe9181de

APP INFORMATION

App Name Undangan Digital
Package Name com.google.androidsmstesT
Main Activity com.example.myapplication.MainActivity
Target SDK 32 Min SDK 26 Max SDK
Android Version Name 1.0 Android Version Code 1

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|---|---|---|
| android.permission.INTERNET | normal | full Internet access | Allows an application to create network sockets. |
| android.permission.READ_SMS | dangerous | read SMS or MMS | Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages. |
| android.permission.RECEIVE_SMS | dangerous | receive SMS | Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you. |
| android.permission.SEND_SMS | dangerous | send SMS messages | Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation. |

Ketika aplikasi tersebut terpasang di perangkat android milik korban, penipu memiliki kemungkinan untuk mengakses data SMS yang mencantumkan informasi SMS-Banking seperti kode pin dari riwayat SMS.

Sebagian besar korban memiliki kemungkinan tidak menghapus Riwayat transaksi dari SMS-banking sehingga dapat mengakibatkan penyerang mendapatkan informasi rahasia dan dapat meminta SMS token secara illegal. Apabila ini dapat dilakukan, penyerang dapat melakukan pengiriman uang dari rekening korban.

## Panduan Mitigasi

- Mengunduh dan menginstal aplikasi hanya dari toko aplikasi resmi, Play Store atau iOS App Store.
- Melakukan pembaruan sistem operasi, aplikasi/software, firmware, dan web browser secara berkala untuk meningkatkan keamanan perangkat dari kerawanan yang ada

- Berhati-hati setiap kali membuka tautan yang didapat.
- Selalu perbarui kata sandi (password) secara berkala.

- Teliti dalam memberikan izin untuk aplikasi yang diinstalasi
- Menggunakan antivirus dan perangkatJ keamanan yang terkini (update) dan lakukan pemindaian antivirus baik terhadap storage dan memory secara berkala.

# REFERENSI


- “Viral File Android Berkedok J&T Express, BSSN: Ini Malware SMS Stealer Kategori Dangerous” https://cyberthreat.id/read/14999/Viral-File-Android-Berkedok-JT-Express-BSSN-Ini-Malware-SMS-Stealer-Kategori-Dangerous (diakses Januari 28, 2023).
- "Awas! File APK Undangan Nikah Bisa Jadi Modus Baru Bobol Rekening, Ini Tips agar Tak Jadi Korban” https://www.kompas.tv/article/372543/awas-file-apk-undangan-nikah-bisa-jadi-modus-baru-bobol-rekening-ini-tips-agar-tak-jadi-korban (diakses Januari 28, 2023).
- “Beredar Aplikasi Android Jahat 'Undangan Pernikahan'. Diduga Masih Satu Geng dengan Malware Kurir” https://cyberthreat.id/read/15287/Beredar-Aplikasi-Android-Jahat-Undangan-Pernikahan-Diduga-Masih-Satu-Geng-dengan-Malware-Kurir (diakses Januari 28, 2023).
- “Android Package Kit (APK) | Definition” https://www.kochava.com/glossary/apk/ (diakses Januari 28, 2023).

# INFORMASI DOKUMEN

## KETENTUAN PENGGUNAAN DOKUMEN

Dokumen Imbauan ini tersedia secara bebas dengan mengakses portal Website ID-SIRTII/CC. Terkait penggunaan dokumen imbauan ini, dapat digunakan oleh seluruh pihak yang menggunakan produk terdampak kerawanan yang diulas pada dokumen imbauan ini.

## RIWAYAT DOKUMEN

| VERSI DOKUMEN | TANGGAL RILIS |
|---|---|
| 1.0 | 28 JANUARI 2023 |

## KONTAK KAMI

DIREKTORAT OPERASI KEAMANAN SIBER
NATIONAL CSIRT OF INDONESIA
Id-SIRTII/CC
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE COORDINATION CENTER

Jl. Harsono RM No. 70, Ragunan, Pasar Minggu, Jakarta Selatan 12550
(021) 788 33610
bantuan70@bssn.go.id


BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
BHINNEKA TUNGGAL IKA
STHANA PAROKSHARTA BHAKTI