09 Februari 2024

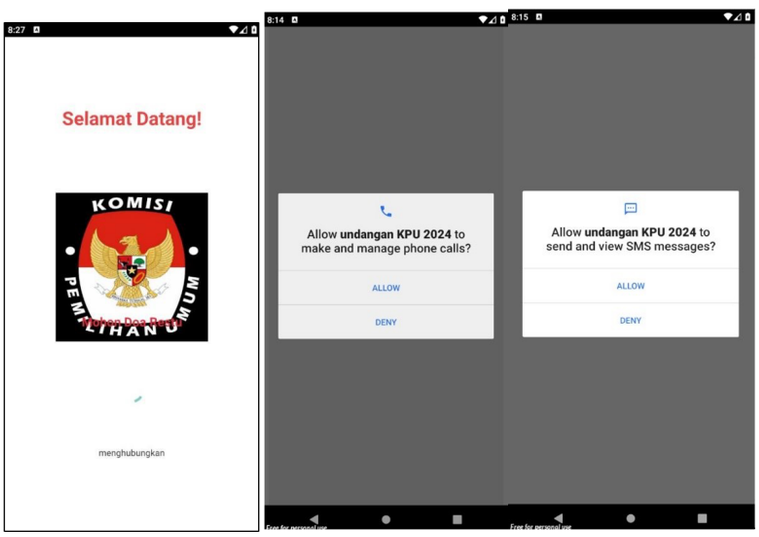
SECURITY ADVISORY
APK PEMILU 2024

Tiga malware yang teridentifikasi berkaitan dengan Pemilu 2024 dengan ekstensi APK menghadirkan ancaman serius terhadap keamanan dan privasi pengguna. Malware tersebut berfungsi untuk mengambil informasi dan kredensial dari perangkat yang terinfeksi. Mirip dengan malware **undanganpernikahan.apk**, salah satu penyebaran ketiga malware tersebut adalah melalui pesan Whatsapp. Serangan ini mencoba mengelabui pengguna untuk mengunduh dokumen palsu yang sebenarnya bertujuan meretas perangkat pribadi. Perlu memastikan untuk tidak mengunduh atau membuka dokumen dari sumber yang tidak dikenal guna melindungi keamanan pribadi dan perangkat pribadi dari potensi serangan malware atau pencurian data.

Nama File	Nilai Hash MD5	Waktu Pembuatan
CEK DATA PEMILIHAN UMUM 2024.APK	b3ea6e4e33c83998d95145b18c2fb6b6	2024-01-31 Pukul 11:51:26
Daftar Pemilu 2024.APK	b3ac745e8386a5d1c79b9f27bb196f34	2023-07-08 Pukul 13:35:30
Simulasi Pemilu Pilpres2024.txt.APK	21487a0c8882a1de3ac74a81598fa912	2024-01-28 Pukul 23:13:08

CEK DATA PEMILIHAN UMUM 2024.APK

Berdasarkan analisis statis, terdapat beberapa temuan informasi yang bersumber pada source code aplikasi **CEK DATA PEMILIHAN UMUM 2024.APK**, seperti permintaan akses berbahaya pada perangkat, bot API Telegram pelaku, dan indikasi nomor telepon pelaku. Perizinan akses tersebut memungkinkan pelaku kejahatan mendapatkan beberapa informasi terkait seperti lokasi perangkat terinfeksi, pesan SMS, dan panggilan perangkat. Berdasarkan analisis dinamis yang telah dilakukan terhadap APK, diketahui bahwa pada saat APK dibuka untuk pertama kali, maka APK akan meminta akses terhadap beberapa permission diantaranya akses ke telepon, pesan SMS, dan notifikasi perangkat.



Gambar 1. Tampilan CEK DATA PEMILIHAN UMUM 2024.APK

Setelah mendapatkan akses terhadap perangkat, maka APK akan menampilkan pesan selamat datang disertai dengan lambang Komisi Pemilihan Umum.

Diterbitkan Oleh
Id-SIRTII/CC
Indonesia Security Incident Response team on Internet Infrastructure Coordination Center

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

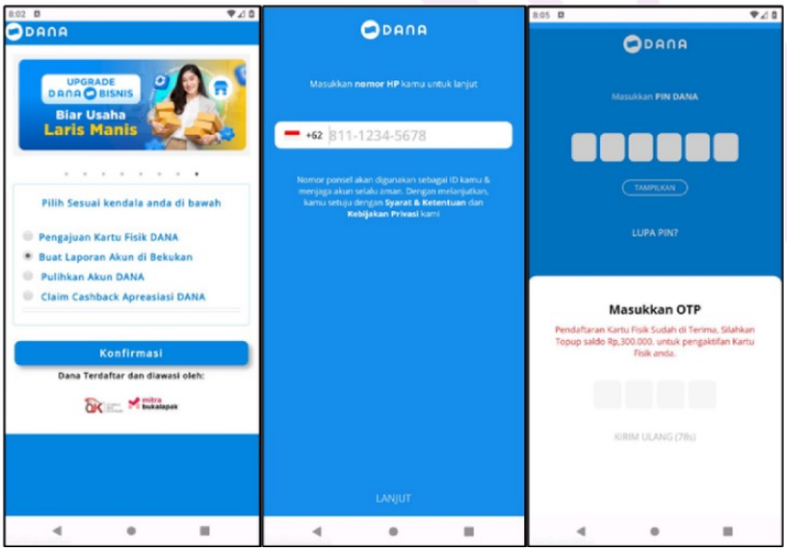
09 Februari 2024

SECURITY ADVISORY

APK PEMILU 2024

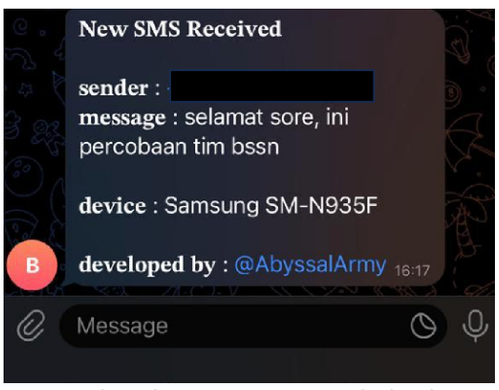
Daftar Pemilu 2024.APK

Berdasarkan analisis statis, terdapat beberapa temuan informasi yang bersumber pada source code aplikasi **Daftar Pemilu 2024.APK**, seperti permintaan akses berbahaya pada perangkat dan bot API Telegram pelaku. Perizinan akses tersebut memungkinkan pelaku kejahatan mendapatkan pesan SMS dan akses internet. Berdasarkan analisis dinamis yang telah dilakukan terhadap APK, diketahui bahwa pada saat APK dibuka, maka menampilkan web phising yang menyerupai interface aplikasi dompet digital DANA dengan tampilan berikut.



Gambar 2. Tampilan Daftar Pemilu 2024.APK

APK berbahaya tersebut mengharuskan pengguna untuk menginputkan nomor telepon dan PIN yang terdaftar di aplikasi dompet digital DANA. Hal ini merupakan cara penyerang untuk mendapatkan informasi berupa nomor telepon dan PIN dari aplikasi DANA korban. Ketika aplikasi diinstal pada perangkat korban, APK berbahaya mengirimkan pemberitahuan kepada penyerang bahwa APK berbahaya telah menginfeksi perangkat korban. Pemberitahuan ini dikirimkan kepada bot telegram penyerang sebagaimana yang ditunjukkan pada gambar. Informasi yang diberitahukan meliputi jenis device yang menginstal malware, serta notifikasi bahwa penyerang sudah dapat membaca isi pesan SMS pada device korban.



Gambar 3. Pencurian data berupa SMS pada korban oleh penyerang

Diterbitkan Oleh

Id-SIRTII/CC

Indonesia Security Incident Response team on Internet Infrastructure Coordination Center

Badan Siber dan Sandi Negara

(021) 788 33610

bantuan70@bssn.go.id

Jl. Harsono RM No. 70, Ragunan, Pasar Minggu, Jakarta Selatan 12550

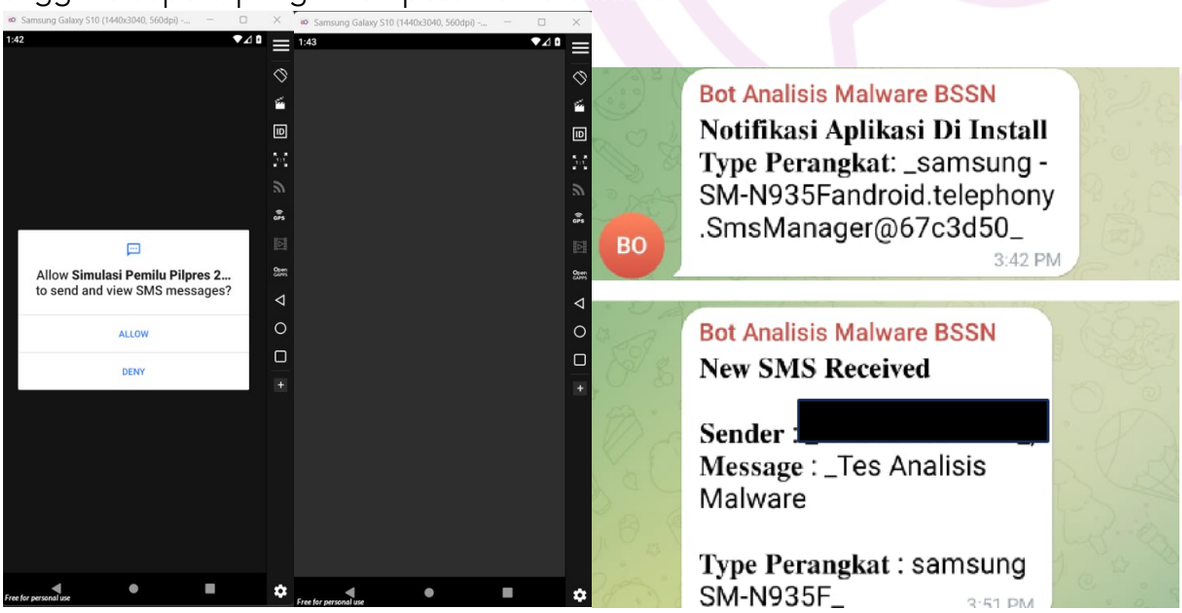
09 Februari 2024

SECURITY ADVISORY

APK PEMILU 2024

Simulasi Pemilu Pilpres2024.txt.APK

Berdasarkan analisis dinamis yang telah dilakukan, diketahui bahwa pada saat APK dibuka untuk pertama kali, maka APK akan meminta akses terhadap beberapa permission diantaranya mengirim dan melihat SMS, dan semua notifikasi perangkat. Ketika berhasil dilakukan instalasi, aplikasi tidak mengarahkan ke link yang berhubungan ke Pemilu 2024 (hanya menampilkan layar hitam) sementara pelaku sudah berhasil mencuri informasi pengguna seperti pengiriman pesan SMS berikut



Gambar 4. Tampilan Simulasi Pemilu Pilpres2024.txt.APK dan Pencurian data berupa SMS pada korban oleh penyerang

Langkah Mitigasi

- Mengunduh dan menginstal aplikasi hanya dari official app store seperti Play Store atau iOS App Store
- Melakukan update Operating System, Aplikasi/Software, Firmware dan Browser secara berkala untuk meningkatkan keamanan perangkat dari kerawanan yang ada
- Teliti dalam memberikan ijin untuk aplikasi yang diinstalasi
- Berhati-hati setiap kali membuka tautan/link yang didapatkan
- Selalu update password secara berkala.
- Menggunakan antivirus dan perangkat security yang update dan lakukan scanning antivirus baik terhadap storage dan memory secara berkala;

Produk Terancam

- Pengguna Android

Diterbitkan Oleh
Id-SIRTII/CC
Indonesia Security Incident Response team on Internet Infrastructure Coordination Center

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

09 Februari 2024

SECURITY ADVISORY

APK PEMILU 2024

Referensi Lanjutan, Solusi, dan Alat

- https://www.virustotal.com/gui/file/99b1c441583d21b61fc6f870b0085a69ae99a107485e1c4f7c8752022151a19b
- https://www.virustotal.com/gui/file/bdb22462b7f7d8c216d462a4630d8a1f627ea1916836812ff778232376f8d00c
- https://www.virustotal.com/gui/file/2e79a1c4898e678367d23af333b767b7759c6d1c3f1745d4ee52dfa6f098d6af
- https://www.idsirtii.or.id/berita/baca/952/malware-undangan-pernikahan.html
- Laporan analisis malware : APK Pemilu 2024

Informasi Imbauan Keamanan Lainnya di laman **Id-SIRTII/CC**

https://www.idsirtii.or.id/peringatan.html

Sumber Penulisan

- [Diakses 09 Februari 2024] https://cwe.mitre.org/data/definitions/284.html
- Laporan Analisis Malware Tim BSSN

Diterbitkan Oleh

Id-SIRTII/CC

Indonesia Security Incident Response team on Internet Infrastructure Coordination Center

Badan Siber dan Sandi Negara

(021) 788 33610

bantuan70@bssn.go.id

Jl. Harsono RM No. 70, Ragunan, Pasar Minggu, Jakarta Selatan 12550