Laporan Aktifitas Malware : reptilicus

Tanggal : 26 September 2024

Waktu Mulai : 14.18 WIB

Waktu Selesai :

Nama Malware :

Jenis Analisis : Statis

1. Deskripsi Malware
   Reptilicus : Pertahanan Keluarga merupakan aplikasi pengawasan orang tua yang digunakan untuk mengawasi handphone anak nya

2. Metodologi
   Analisis dilakukan dengan metode static yang di operasikan menggunakan MobSF Static Analyzer

3. Aktivitas yang ditemukan
   a. Proses yang dijalankan
      - Proses Utama : Reptilicus. Защита семьи. Официальное приложение.xapk
      - Waktu mulai : 14.20 WIB
      - Aktivitas : meminta perizinan kepada user
   b. Koneksi Jaringan
      - Domain yang terhubung : reptilicus.net
      - Ip address : 188.166.164.158
      - Tipe koneksi : TCP
   c. Persetujuan yang biasanya ada di malware
      - android.permission.ACCESS_NETWORK_STATE
      - android.permission.INTERNET
      - android.permission.WAKE_
   d. Persetujuan yang mencurigakan
      - com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE
      - com.google.android.c2dm.permission.RECEIVE
4. Analisis Perilaku

   Pengamatan : Aplikasi meminta persetujuan pengguna lalu memberikan laporan mengenai kondisi handphone pengguna ke server utama dan akan di padahalaman dashboard admin

   Tindakan Berbahaya : Aplikasi reptilicus dapat digunakan untuk menguntit orang yang tidak mengerti tentang teknologi, bahkan dapat mencari informasi sensitif di dalam handphone pengguna

5. Kesimpulan

   Aplikasi reptilicus merupakan aplikasi pemantau yang dapat digunakan oleh orang tua untuk mengelola handphone yang anak mereka punya, tetapi dapat digunakan pula oleh peretas jahat untuk menyusup lalu mendapatkan hak akses penuh ke korban dan mencuri informasi sensitif

6. Rekomendasi
   a. Segera hapus jika pengguna tidak sadar menginstall aplikasi reptilicus
   b. Segera ganti semua password/akses masuk dan terapkan 2MFA