Laporan Aktifitas Malware : reptilicus

Tanggal : 26 September 2024

Waktu Mulai : 14.18 WIB

Waktu Selesai : 14.32 WIB

Nama Malware : reptilicus

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 : net.reptilicus.mainappl
      - Waktu mulai : 14.19 WIB
      - Aktivitas : meminta perizinan pengguna

   b. Koneksi Jaringan
      - Domain 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_LOCK

   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. Jika ditemukan pada perangkat, segera lakukan pemindaian dengan perangkat lunak anti-malware atau anti-spyware untuk mendeteksi dan menghapus spyware ini.
   b. Aktifkan autentikasi dua faktor (2FA) dan gunakan kata sandi yang kuat untuk mencegah akses tidak sah.