Laporan Aktifitas Malware : ZoeMob

Tanggal : 03 Oktober 2024

Waktu Mulai : 16.30 WIB

Waktu Selesai : 16.59 WIB

Nama Malware : ZoeMob

Jenis Analisis : Statis

1. Deskripsi Malware

   ZoeMob merupakan spyware yang dibuat untuk orang tua memantau/mengawasi loksi keberadaan handphone anak mereka lewat gps dengan Tingkat akurasi yang detail
2. Metodologi

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

3. Aktivitas yang ditemukan
   a. Proses yang dijalankan
      - Proses utama : com.zoemob.gpstracking
      - Waktu mulai : 16.32 WIB
      - Aktivitas : Meminta perizinan GPS ke pengguna

   b. Koneksi Jaringan
      - Domain terhubung : data.flurry.com
      - Ip address : 106.10.248.147
      - Tipe koneksi : TCP

   c. Persetujuan yang biasanya ada di malware
      - android.permission.READ_CONTACTS,
      - android.permission.READ_PHONE_STATE, android.permission.VIBRATE,
      - android.permission.INTERNET,
      - android.permission.ACCESS_NETWORK_STATE,
      - android.permission.ACCESS_WIFI_STATE,
      - android.permission.ACCESS_COARSE_LOCATION,
      - android.permission.ACCESS_FINE_LOCATION,
      - android.permission.WAKE_LOCK,
      - android.permission.RECEIVE_BOOT_COMPLETED,
      - android.permission.WRITE_EXTERNAL_STORAGE,
      - android.permission.GET_ACCOUNTS, android.permission.GET_TASKS,
      - android.permission.READ_EXTERNAL_STORAGE

   d. Persetujuan yang mencurigakan
      - android.permission.CALL_PHONE, android.permission.WRITE_CONTACTS,
      - android.permission.CHANGE_NETWORK_STATE,

- android.permission.CHANGE_WIFI_STATE,
- android.permission.ACCESS_BACKGROUND_LOCATION,
- android.permission.FOREGROUND_SERVICE,
- com.google.android.c2dm.permission.RECEIVE,
- com.google.android.gms.permission.ACTIVITY_RECOGNITION,
- android.permission.ACTIVITY_RECOGNITION

4. Analisis Perilaku

   Pengamatan : ZoeMob akan melacak Lokasi keberadaan handphone milik anak mereka melalui gps dan Lokasi yang ditampilkan itu real-time

   Tindakan berbahaya : ZoeMob dapat disalahgunakan oleh orang yang ingin menguntit atau memata-matai orang lain

5. Kesimpulan

   ZoeMob merupakan aplikasi yang dibuat untuk melacak ponsel milik anak-anak, tetapi aplikasi ini juga dapat digunakan untuk menguntit orang lain

6. Rekomendasi
   a. Segera hapus jika pengguna tidak sadar menginstall aplikasi ZoeMob
   b. Minta tolong orang yang mahir dibidang ini untuk menghapus aplikasi ini
   c. Segera ganti semua password/akses masuk dan terapkan 2MFA