Laporan Aktifitas Malware : uMobix

Tanggal : 30 September 2024

Waktu Mulai : 10.11 WIB

Waktu Selesai : 10.26 WIB

Nama Malware : uMobix

Jenis Analisis : Statis

1. Deskripsi Malware
   uMobix merupakan spyware yang dibuat untuk orang tua memantau/mengawasi kegiatan handphone anak mereka seperti kegiatan sosial media, isi gallery, isi nomor kontak, informasi tentang handphone mereka

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

3. Aktivitas yang ditemukan
   a. Proses yang dijalankan
      - Proses utama : umobix-1-0-0.apk
      - Waktu mulai : 10.15 WIB
      - Aktivitas : meminta perizinan pengguna

   b. Koneksi Jaringan
      - Domain terhubung : api.taboola.com
      - Ip address : 199.232.45.44
      - Tipe koneksi : TCP

   c. Persetujuan yang biasanya ada di malware
      - android.permission.ACCESS_WIFI_STATE,
      - android.permission.ACCESS_NETWORK_STATE,
      - android.permission.ACCESS_FINE_LOCATION,
      - android.permission.ACCESS_COARSE_LOCATION,
      - android.permission.INTERNET

   d. Persetujuan yang mencurigakan
      - android.permission.CHANGE_WIFI_STATE,
      - com.google.android.gms.permission.AD_ID

4. Analisis Perilaku
   Pengamatan : uMobix akan meminta perizianan pengguna seperti jaringan dan gps untuk memantau Lokasi akurat handphone anak mereka berada. Dan spyware ini juga bisa menampilkan iklan dalam full-screen sehingga dapat mengganggu pengguna nya

   Tindakan berbahaya : uMobix bisa saja memasukkan iklan yang terinfeksi malware kedalam handphone pengguna

5. Kesimpulan
   uMobix merupakan malware yang tujuan utamanya untuk orang tua mengawasi handphone anak mereka, tapi dalam aplikasi uMobix ini ada indikasi dapat menampilkan iklan yang dapat mengganggu kinerja handphone pengguna

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