Laporan Aktifitas Malware : LockItTight

Tanggal : 07 Oktober 2024

Waktu Mulai : 10.07 WIB

Waktu Selesai : 10.30 WIB

Nama Malware : LockItTight

Jenis Analisis : Statis

1. Deskripsi Malware

   LockItTight merupakan spyware yang dibuat dengan tujuan supaya pengguna dapat mengakses/mengendalikan handphone nya dari jarak jauh, aplikasi ini juga bisa menjadi Solusi untuk orang tua mengendalikan ponsel anaknya
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.timeon.litclient
      - Waktu mulai : 10.08 WIB
      - Aktivitas : Meminta perizinan pengguna

   b. Koneksi Jaringan
      - Domain terhubung : dev.lockittight.com
      - Ip address : 76.176.108.212
      - Tipe koneksi : TCP

   c. Persetujuan yang biasanya ada di malware
      - android.permission.INTERNET,
      - android.permission.ACCESS_NETWORK_STATE,
      - android.permission.ACCESS_WIFI_STATE,
      - android.permission.READ_PHONE_STATE,
      - android.permission.ACCESS_FINE_LOCATION,
      - android.permission.RECEIVE_BOOT_COMPLETED,
      - android.permission.READ_EXTERNAL_STORAGE,
      - android.permission.CAMERA

   d. Persetujuan yang mencurigakan
      - android.permission.CHANGE_WIFI_STATE

4. Analisis Perilaku

   Pengamatan : LockItTight akan meminta perizinan pengguna seperti jaringan gan gps untuk memantau Lokasi akurat handphone pengguna berada

   Tindakan berbahaya : aplikasi ini memiliki fitur persistent yang sulit untuk di hapus
5. Kesimpulan

   LockItTight merupakan spyware yang tujuan utamanya untuk orang tua mengawasi ponsel pengguna nya tetapi dapat di salah gunakan

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