Laporan Aktifitas Malware : letmespy

Tanggal : 26 September 2024

Waktu Mulai : 16.17 WIB

Waktu Selesai : 16.40 WIB

Nama Malware : letmespy

Jenis Analisis : Statis

1. Deskripsi Malware

   Letmespy.apk merupakan aplikasi spyware yang dapat mencadangkan SMS, log telepon, dan Lokasi handphone secara luring selama handphone masih terkoneksi dengan internet

2. Metodologi

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

3. Aktivitas yang ditemukan
   a. Proses yang dijalankan
      - Proses Utama : pl-lidwin-letmespy.apk
      - Waktu mulai : 16.19 WIB
      - Aktivitas : Menghubungi server controller

   b. Koneksi Jaringan
      - Domain terhubung : letmespy.com, www.teleszpieg.pl
      - Ip address : 36.86.63.185, 2.168.1.110
      - Tipe Koneksi : TCP

   c. Persetujuan yang biasanya ada di malware
      - android.permission.INTERNET, android.permission.READ_SMS,
      - android.permission.RECEIVE_SMS,
      - android.permission.RECEIVE_BOOT_COMPLETED,
      - android.permission.READ_CALL_LOG,
      - android.permission.READ_CONTACTS,
      - android.permission.ACCESS_FINE_LOCATION
      - android.permission.ACCESS_COARSE_LOCATION
      - android.permission.GET_ACCOUNTS
      - android.permission.WAKE_LOCK,
      - android.permission.RECORD_AUDIO
      - android.permission.WRITE_EXTERNAL_STORAGE

   d. Persetujuan yang mencurigakan
      - android.permission.PROCESS_OUTGOING_CALLS,
      - com.google.android.c2dm.permission.RECEIVE

4. Analisis Perilaku
    a. Aplikasi berjalan dilatar belakang dan tidak bisa dihentikan
    b. Aplikasi mengumpulkan data seperti log telepon dan sms
    c. Aplikasi dapat melacak dalam waktu yang sama persis asalkan handphone terhubung dengan internet
    d. Data yang dikumpulkan dapat di ambil secara luring melalui situs tertentu

5. Kesimpulan

    Letmespy ini memiliki kemampuan untuk secara diam-diam mengumpulkan informasi sensitif seperti panggilan telepon, pesan, dan lokasi pengguna tanpa sepengetahuan mereka. Meskipun aplikasi ini menyertakan fitur kontrol untuk menghentikan pengumpulan data dan mengklaim memiliki tujuan etis, seperti melacak perangkat yang hilang, kemampuannya berjalan di latar belakang dan mengirim data ke server eksternal menimbulkan risiko besar bagi privasi. Penyalahgunaan aplikasi ini sangat mungkin terjadi untuk tujuan penguntitan atau pelanggaran privasi, menjadikannya ancaman serius jika digunakan tanpa izin yang jelas dari pengguna perangkat.

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.