Laporan Aktifitas Malware : Call Recorder – Talk Log

Tanggal : 1 Oktober 2024

Waktu Mulai : 10.27 WIB

Waktu Selesai : 10.50 WIB

Nama Malware : Call Recorder – Talk Log

Jenis Analisis : Statis

1. Deskripsi Malware

   Talklog merupakan aplikasi yang digunakan untuk merekam pembicaraan telepon, dapat di aktifkan lewat beberapa cara contoh nya melalui timer atau digoyangkan

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.wdroid.paranoid
      - Waktu mulai : 10.29 WIB
      - Aktivitas : meminta perizinan pengguna

   b. Koneksi Jaringan
      - Domain terhubung : talklog.net
      - Ip address : 172.67.193.75
      - Tipe koneksi : TCP

   c. Persetujuan yang biasanya ada di malware
      - android.permission.INTERNET, android.permission.RECORD_AUDIO,
      - android.permission.VIBRATE, android.permission.WAKE_LOCK,
      - android.permission.SYSTEM_ALERT_WINDOW,
      - android.permission.ACCESS_NETWORK_STATE

   d. Persetujuan yang mencurigakan
      - android.permission.FOREGROUND_SERVICE,
      - android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS,
      - com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE,
      - com.google.android.c2dm.permission.RECEIVE

4. Analisis Perilaku
   Pengamatan : Aplikasi TalkLog akan merekam pembicaraan telepon, mau itu whatsapp ataupun seluler dan menyimpan nya di penyimpanan internal

   Tindakan berbahaya : Aplikasi TalkLog bisa saja diam-diam mengirim data rekaman pengguna ke server mereka

5. Kesimpulan
   Aplikasi TalkLog bisa dikatakan aplikasi biasa saja, namun memiliki fitur yang cukup beresiko pada privasi pengguna

6. Rekomendasi
   - Gunakan aplikasi TalkLog jika menerima panggilan dari nomor yang tidak di kenal
   - Jika merasa tidak nyaman, lebih baik dihapus saja aplikasi TalkLog