Laporan Aktifitas Malware : SeekDroid

Tanggal : 05 Oktober 2024

Waktu Mulai : 15.23 WIB

Waktu Selesai : 15.45 WIB

Nama Malware : SeekDroid

Jenis Analisis : Statis

1. Deskripsi Malware

   SeekDroid merupakan aplikasi spyware yang dibuat untuk tujuan pengguna melacak ponsel pengguna jika hilang dan menghapus data nya dari jarak jauh jika diperlukan
2. Metodologi

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

3. Aktivitas yang ditemukan
   a. Proses yang dijalankan
      - Proses utama : org.gtmedia.seekdroid
      - Waktu mulai : 15.25
      - Aktivitas : meminta perizinan pengguna

   b. Koneksi Jaringan
      - Domain terhubung : help.seekdroid.com
      - Ip address : 23.235.226.110
      - Tipe koneksi : TCP

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

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

4. Analisis Perilaku

   Pengamatan : SeekDroid dapat melacak Lokasi akurat ponsel selama ponsel memiliki akses koneksi internet dan ponsel dalam keadaan hidup

   Tindakan berbahaya : SeekDroid dapat menjadi aplikasi yang berguna bagi penjahat untuk memata-matai seseorang

5. Kesimpulan

   SeekDroid merupakan aplikasi yang dibuat untuk melacak ponsel yang hilang, tetapi SeekDroid juga dapat digunakan penjahat untuk memata-matai seseorang

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