Laporan Aktifitas Malware : SpyDroid

Tanggal : 03 Oktober 2024

Waktu Mulai : 10.50 WIB

Waktu Selesai : 11.17 WIB

Nama Malware : SpyDroid

Jenis Analisis : Statis

1. Deskripsi Malware

   SpyDroid merupakan spyware yang dibuat untuk ‘prank’ tetapi fitur yang diberikan memiliki dampak yang cukup parah seperti bisa melihat kamera depan atau belakang, melihat stream layar ponsel pengguna, menggetarkan ponsel
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.majorkernelpanic.spydroid
      - Waktu mulai : 10.52 WIB
      - Aktivitas : meminta perizinan pengguna

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

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

   d. Persetujuan yang mencurigakan
      - -

4. Analisis Perilaku

   Pengamatan : SpyDroid merupakan aplikasi yang dapat membuat stream layar ponsel atau web browser pengguna ke dalam VLC

Tindakan berbahaya : SpyDroid dapat berbahaya jika berhasil di eksploitasi oleh penjahat

5. Kesimpulan

   SpyDroid merupakan aplikasi yang awalnya hanya untuk ‘prank’ tapi dapat digunakan untuk kegiatan illegal

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