Laporan Aktifitas Malware : SpyFly

Tanggal : 02 Oktober 2024

Waktu Mulai : 17.07 WIB

Waktu Selesai : 17.35 WIB

Nama Malware : SpyFly

Jenis Analisis : Statis

1. Deskripsi Malware

   SpyFly merupakan spyware untuk memantau orang lain, aplikasi SpyFly ini berjalan di latar belakang dan bisa mereka pembicaraan, akses dari jauh, menyimpan telpon/sms, dan dapat mengetahui lokasi akurat penggguna

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.spyfly.spyflyapp
      - Waktu mulai : 17.10 WIB
      - Aktivitas : meminta peqrizinan pengguna

   b. Koneksi Jaringan
      - Domain terhubung : spyfly-160413.firebaseio.com
      - Ip address : 34.120.206.254
      - Tipe koneksi : TCP

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

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

4. Analisis Perilaku

   Pengataman : SpyFly akan meminta perizinan pengguna untuk akses direktori, catatan telepon, sms, notifikasi, dan Lokasi detail. Lalu aplikasi akan menghapus icon/shortcut aplikasi nya

   Tindakan berbahaya : SpyFly dapat menjadi aplikasi berbahaya jika digunakan oleh pihak yang tidak bertanggung jawab atau disalah gunakan

5. Kesimpulan

   SpyFly merupakan aplikasi yang memang dibuat untuk tujuan memata-matai orang demi keuntungan pribadi

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