Laporan Aktifitas Malware : SpyPhoneApp

Tanggal : 30 September 2024

Waktu Mulai : 13.31 WIB

Waktu Selesai : 13.54 WIB

Nama Malware : SpyPhoneApp

Jenis Analisis : Statis

1. Deskripsi Malware

   SpyPhoneApp merupakan spyware yang dibuat dengan tujuan untuk memantau orang berasangkutan seperti anak-anak atau karyawan. SpyPhoneApp juga dapat membuat backup dari jarak jauh

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.sptrakapp.alarm
      - Waktu mulai : 13.35 WIB
      - Aktivitas : meminta perizinan pengguna

   b. Koneksi Jaringan
      - Domain terhubung : appr.tc
      - Ip address : 216.239.38.21
      - Tipe koneksi : TCP

   c. Persetujuan yang biasanya ada di malware
      - android.permission.INTERNET,
      - android.permission.WRITE_EXTERNAL_STORAGE,
      - android.permission.READ_PHONE_STATE, android.permission.RECEIVE_SMS,
      - android.permission.READ_SMS,
      - android.permission.ACCESS_COARSE_LOCATION,
      - android.permission.RECORD_AUDIO,
      - android.permission.READ_EXTERNAL_STORAGE,
      - android.permission.ACCESS_NETWORK_STATE,
      - android.permission.READ_CALL_LOG, android.permission.READ_CONTACTS,
      - android.permission.ACCESS_FINE_LOCATION,
      - android.permission.RECEIVE_BOOT_COMPLETED,
      - android.permission.CAMERA, android.permission.GET_TASKS,
      - android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE,
      - android.permission.SYSTEM_ALERT_WINDOW

d. Persetujuan yang mencurigakan
    - android.permission.CHANGE_WIFI_STATE,
    - android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS,
    - android.permission.READ_CALENDAR,
    - android.permission.PROCESS_OUTGOING_CALLS,
    - android.permission.FOREGROUND_SERVICE,
    - android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN,
    - android.permission.MODIFY_AUDIO_SETTINGS,
    - android.permission.ACCESS_BACKGROUND_LOCATION,
    - android.permission.FLASHLIGHT, android.permission.BROADCAST_STICKY,
    - android.permission.PACKAGE_USAGE_STATS,
    - com.google.android.c2dm.permission.RECEIVE

4. Analisis Perilaku
   Pengamatan : aplikasi SpyPhoneApp meminta banyak perizinan kepada user untuk berfungsi sempurna

   Tindakan berbahaya : karena banyak sekali perizinan yang diminta, jadi sangat berbahaya jika aplikasi SpyPhoneApp jika disalah gunakan

5. Kesimpulan
   SpyPhoneApp merupakan aplikasi untuk memantau orang dengan persetujuan orang yang bersangkutan

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