Laporan Aktifitas Malware : EasyPhoneTrack

Tanggal : 02 Oktober 2024

Waktu Mulai : 11.32 WIB

Waktu Selesai : 12.05 WIB

Nama Malware : EasyPhoneTrack

Jenis Analisis : Statis

1. Deskripsi Malware

   EasyPhoneTrack merupakan spyware yang ditujukan untuk memantau orang dengan fitur yang canggih seperti Lokasi detail, akses remote, catatan sms dan telepon

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.spappm_mondow.alarm
      - Waktu mulai : 11.34 WIB
      - Aktivitas : meminta perizanan pengguna

   b. Koneksi Jaringan
      - Domain terhubung : www.spy-datacenter.com
      - Ip address : 50.28.38.175
      - 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.RECEIVE_BOOT_COMPLETED,
      - android.permission.READ_CONTACTS,
      - android.permission.ACCESS_FINE_LOCATION,
      - android.permission.ACCESS_COARSE_LOCATION,
      - android.permission.GET_ACCOUNTS,
      - android.permission.ACCESS_WIFI_STATE,
      - android.permission.ACCESS_NETWORK_STATE,
      - android.permission.RECORD_AUDIO,
      - android.permission.READ_EXTERNAL_STORAGE,
      - android.permission.READ_CALL_LOG, android.permission.CAMERA,

- android.permission.GET_TASKS, android.permission.WAKE_LOCK

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

4. Analisis Perilaku

    Pengamatan : EasyPhoneTrack memiliki fitur untuk memata-matai dan mengendalikan ponsel dari jarak jauh, memonitor galery, social media, dan telepon, juga bisa melihat Lokasi detail pengguna

    Tindakan berbahaya : EasyPhoneTrack bisa menjadi aplikasi yang sangat berbahaya jika disalahgunakan karena pengguna tidak akan sadar ada aplikasi pemantau di ponsel nya

5. Kesimpulan

    EasyPhoneTrack merupakan aplikasi yang dibuat dengan tujuan memantau orang yang bersangkutan dan menyetujui, aplikasi ini dapat sangat mudah untuk disalahgunakan untuk kegiatan kejahatan

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