Laporan Aktifitas Malware : MobileSpy.io.io

Tanggal : 02 Oktober

Waktu Mulai : 10.02 WIB

Waktu Selesai : 10.22 WIB

Nama Malware : MobileSpy.io

Jenis Analisis : Statis

1. Deskripsi Malware
   MobileSpy.io merupakan aplikasi spyware pemantau berbayar yang ditujukan untuk memantau anak-anak atau orang tertentu secara sah

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.MobileSpy.io.io
      - Waktu mulai : 10.04 WIB
      - Aktivitas : Meminta perizinan pengguna

   b. Koneksi Jaringan
      - Domain terhubung : admin.MobileSpy.io.io
      - Ip address : 104.21.79.37
      - Tipe koneksi : TCP

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

d. Persetujuan yang mencurigakan
    - android.permission.FOREGROUND_SERVICE,
    - android.permission.PACKAGE_USAGE_STATS,
    - android.permission.WRITE_CONTACTS,
    - android.permission.PROCESS_OUTGOING_CALLS,
    - android.permission.AUTHENTICATE_ACCOUNTS,
    - android.permission.CHANGE_WIFI_STATE,
    - android.permission.ACCESS_BACKGROUND_LOCATION,
    - android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS,
    - android.permission.REQUEST_INSTALL_PACKAGES,
    - com.google.android.c2dm.permission.RECEIVE,
    - com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

4. Analisis Perilaku

    Pengamatan : MobileSpy.io akan meminta perizinan pengguna seperti jaringan gan gps untuk memantau Lokasi akurat handphone anak mereka berada.

    Tindakan berbahaya : aplikasi ini memiliki fitur persistent yang sulit untuk di hapus

5. Kesimpulan

    MobileSpy.io merupakan spyware yang bertujuan untuk memantau penggunaan handphone anak-anak atau orang tertentu, MobileSpy.io juga memiliki fitur yang sangat banyak seperti Lokasi detail, akses remote, monitoring gallery dan sosial media

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