Laporan Aktifitas Malware : WheresMyDroid

Tanggal : 03 Oktober 2024

Waktu Mulai : 13.01 WIB

Waktu Selesai : 13.20 WIB

Nama Malware : WheresMyDroid

Jenis Analisis : Statis

1. Deskripsi Malware

   WheresMyDroid merupakan aplikasi yang dirancang untuk pemilik ponsel melacak keberadaan ponsel nya jika hilang. WheresMyDroid memiliki fitur yang banyak, seperti contohnya melihat Lokasi akurat, menghapus data eksternal/internal ponsel dari jarak jauh, mengunci ponsel 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.alienmanfc6.wheresmyandroid
      - Waktu mulai :
      - Aktivitas : meminta perizinan pengguna

   b. Koneksi Jaringan
      - Domain terhubung : wheresmydroid.com
      - Ip address : 216.239.34.21
      - Tipe koneksi : TCP

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

- android.permission.READ_EXTERNAL_STORAGE

d. Persetujuan yang mencurigakan
    - android.permission.PROCESS_OUTGOING_CALLS,
    - android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS,
    - android.permission.BATTERY_STATS,
    - android.permission.REQUEST_INSTALL_PACKAGES,
    - android.permission.CHANGE_WIFI_STATE,
    - android.permission.CHANGE_NETWORK_STATE,
    - android.permission.FLASHLIGHT,
    - android.permission.MODIFY_AUDIO_SETTINGS,
    - android.permission.FOREGROUND_SERVICE,
    - android.permission.ACCESS_BACKGROUND_LOCATION,
    - com.google.android.gms.permission.ACTIVITY_RECOGNITION,
    - android.permission.ACCESS_NOTIFICATION_POLICY,
    - com.google.android.gms.permission.AD_ID,
    - android.permission.ACTIVITY_RECOGNITION,
    - com.google.android.c2dm.permission.RECEIVE,
    - com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

4. Analisis Perilaku

    Pengamatan : WheresMyDroid awalnya akan meminta perizinan pengguna seperti kontak, sms, gps, wifi, kamera, penyimpanan. Lalu pengguna dapat mengendalikan ponsel lewat halaman admin website

    Tindakan berbahaya : apabila WheresMyDroid terinstall di ponsel orang lain tanpa sepengetahuan nya, maka aplikasi ini dapat mengancam hak akses pemilik ponsel dan bahkan menghapus semua data diam-diam dari jarak jauh

5. Kesimpulan

    WheresMyDroid merupakan aplikasi yang diciptakan untuk pemilik handphone melacak handphone nya jika kehilangan, tetapi aplikasi ini dapat disalahgunakan oleh penjahat

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