Laporan Aktifitas Malware : Spymug

Tanggal : 1 Oktober 2024

Waktu Mulai : 11.14 WIB

Waktu Selesai : 11.39 WIB

Nama Malware : Spymug

Jenis Analisis : Statis

1. Deskripsi Malware
   SpyMug adalah perangkat lunak yang membuat tugas Anda lebih mudah dan Anda dapat mengakses data telepon anak atau pasangan Anda secara efisien. Aplikasi ini menyediakan fasilitas seperti mengekstrak musik, video, dan galeri foto

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.service.mug
      - Waktu mulai : 11.16 WIB
      - Aktivitas : Meminta perizinan pengguna

   b. Koneksi Jaringan
      - Domain terhubung : spymug.com, phonetracking-dd226.firebaseio.com
      - Ip address : 203.161.57.64, 35.190.39.113
      - Tipe koneksi : TCP

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

   d. Persetujuan yang mencurigakan
      - android.permission.CHANGE_WIFI_STATE,
      - android.permission.PROCESS_OUTGOING_CALLS,

- com.google.android.c2dm.permission.RECEIVE

4. Analisis Perilaku

   Pengamatan : Aplikasi meminta persetujuan pengguna lalu memberikan laporan mengenai kondisi handphone pengguna ke server utama dan akan di tampilkan pada halaman dashboard admin

   Tindakan Berbahaya : Aplikasi Spymug dapat digunakan untuk menguntit orang yang tidak mengerti tentang teknologi, bahkan dapat mencari informasi sensitif di dalam handphone pengguna

5. Kesimpulan

   Aplikasi AndroidLost dirancang untuk kegiatan mematai orang secara tidak sah

6. Rekomendasi
   a. Segera hapus jika pengguna tidak sadar menginstall aplikasi Spymug
   b. Segera ganti semua password/akses masuk dan terapkan 2MFA