Laporan Aktifitas Malware : Clevguard

Tanggal : 30 September 2024

Waktu Mulai : 11.35 WIB

Waktu Selesai : 12.03 WIB

Nama Malware : Clevguard

Jenis Analisis : Statis

1. Deskripsi Malware

   Clevguard merupakan spyware yang dibuat untuk orang tua memantau/mengawasi kegiatan handphone anak mereka seperti kegiatan sosial media, isi gallery, isi nomor kontak, informasi tentang handphone mereka

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.clevguard.guard
      - Waktu mulai : 11.37
      - Aktivitas : meminta perizinan pengguna

   b. Koneksi Jaringan
      - Domain terhubung : clevguard.net
      - Ip address : clevguard.net
      - Tipe koneksi : TCP

   c. Persetujuan yang biasanya ada di malware
      - android.permission.ACCESS_NETWORK_STATE,
      - android.permission.READ_EXTERNAL_STORAGE,
      - android.permission.WRITE_EXTERNAL_STORAGE,
      - android.permission.INTERNET,
      - android.permission.SYSTEM_ALERT_WINDOW,
      - android.permission.WAKE_LOCK,
      - android.permission.RECEIVE_BOOT_COMPLETED,
      - android.permission.ACCESS_WIFI_STATE,
      - android.permission.READ_PHONE_STATE

d. Persetujuan yang mencurigakan
    - android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS,
    - android.permission.PACKAGE_USAGE_STATS,
    - com.google.android.gms.permission.AD_ID,
    - android.permission.FOREGROUND_SERVICE,
    - com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

4. Analisis Perilaku

    Pengamatan : Clevguard 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

    Clevguard merupakan malware yang tujuan utamanya untuk orang tua mengawasi handphone anak mereka

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