Laporan Aktifitas Malware : AndroidLost

Tanggal : 27 September 2024

Waktu Mulai : 13.55 WIB

Waktu Selesai : 14.23 WIB

Nama Malware : AndroidLost

Jenis Analisis : Statis

1. Deskripsi Malware

2. Metodologi

   Analisis dilakukan dengan metode static yang di operasikan menggunakan MobSF Static Analyzer

3. Aktivitas yang ditemukan
   a. Proses yang dijalankan
      - Proses utama : lost-android-4-0-177.apk
      - Waktu mulai : 13.56
      - Aktivitas : Meminta perizinan pengguna dan mengecek akses root

   b. Koneksi Jaringan
      - Domain terhubung : www.androidlost.com, proxy.androidlost.com
      - Ip address : 216.239.32.21, 144.76.174.115
      - Tipe koneksi : TCP

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

   d. Persetujuan yang mencurigakan
      - android.permission.ACCESS_BACKGROUND_LOCATION,
      - android.permission.ACCESS_NOTIFICATION_POLICY,
      - android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN,
      - android.permission.CALL_PHONE,

- android.permission.CHANGE_NETWORK_STATE,
- android.permission.CHANGE_WIFI_STATE, android.permission.FLASHLIGHT,
- android.permission.FOREGROUND_SERVICE,
- android.permission.MODIFY_AUDIO_SETTINGS,
- android.permission.REQUEST_INSTALL_PACKAGES,
- 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 AndroidLost 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 TheTruthSpy
   b. Segera ganti semua password/akses masuk dan terapkan 2MFA