Laporan Aktifitas Malware : PanSpy

Tanggal : 27 September 2024

Waktu Mulai : 13.37 WIB

Waktu Selesai : 13.55 WIB

Nama Malware : PanSpy

Jenis Analisis : Statis

1. Deskripsi Malware
   PanSpy merupakan spyware yang dibuat dengan tujuan sebagai aplikasi *parental control* Untuk anak 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.panspy.android
      - Waktu : 13.41
      - Aktivitas : meminta perizinan pengguna

   b. Koneksi Jaringan
      Domain terhubung : s1.panspy.com, www.jivesoftware.com
      Ip address : 47.254.91.221, 23.235.209.143
      Tipe koneksi : TCP

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

d. Persetujuan yang mencurigakan
    - android.permission.ACCESS_BACKGROUND_LOCATION,
    - android.permission.PROCESS_OUTGOING_CALLS,
    - android.permission.WRITE_CONTACTS, android.permission.WRITE_SMS,
    - android.permission.READ_CALENDAR,
    - android.permission.PACKAGE_USAGE_STATS,
    - android.permission.BLUETOOTH,
    - android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS,
    - android.permission.REQUEST_INSTALL_PACKAGES,
    - android.permission.CALL_PHONE,
    - android.permission.FOREGROUND_SERVICE,
    - com.google.android.c2dm.permission.RECEIVE,
    - com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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 ini dapat disalah gunakan untuk mematai orang lain yang tidak terikat/terkait

5. Kesimpulan

    Aplikasi PanSpy merupakan aplikasi pemantau yang dapat digunakan oleh orang tua untuk mengelola handphone yang anak mereka punya, tetapi dapat digunakan pula oleh peretas jahat untuk menyusup lalu mendapatkan hak akses penuh ke korban dan mencuri informasi sensitif

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