Laporan Aktifitas Malware : FlexiSpy

Tanggal : 27 September 2024

Waktu Mulai : 10.29 WIB

Waktu Selesai : 10.50 WIB

Nama Malware : FlexiSpy

Jenis Analisis : Statis

1. Deskripsi Malware
   Flexispy merupakan malware berjenis spyware yang digunakan bertujuan untuk memantau orang. Pada laman website resmi nya, flexispy mengatakan bahwa flexispy dapat digunakan untuk memantau karyawan secara efektif tanpa ketahuan

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.husnain.flexispypro
      - Waktu mulai : 09.00
      - Aktivitas : Mengecek apakah handphone sudah di root atau belum

   b. Koneksi Jaringan
      - Domain yang terhubung : corp.aarki.com
      - Ip address : 204.130.244.41
      - Tipe koneksi : TCP

   c. Persetujuan yang biasanya ada di malware
      - android.permission.INTERNET, android.permission.ACCESS_FINE_LOCATION,
      - android.permission.ACCESS_WIFI_STATE,
      - android.permission.ACCESS_COARSE_LOCATION,
      - android.permission.ACCESS_NETWORK_STATE,
      - android.permission.WAKE_LOCK

   d. Persetujuan yang mencurigakan
      - android.permission.CHANGE_WIFI_STATE,
      - com.google.android.gms.permission.AD_ID,
      - android.permission.FOREGROUND_SERVICE

4. Analisis Perilaku

   Pengamatan : Aplikasi meminta berbagai maca perizinan atas kendali handphone, lalu mengecek apakah handphone sudah dalam keadaan *root* atau belum, jika sudah dalam keadaan root maka aplikasi FlexiSpy dapat menyamarkan diri nya

   Tindakan Berbahaya : Aplikasi FlexiSpy dapat menyamarkan dirinya secara tersembunyi setelah mendeteksi perangkat yang telah di-root, memungkinkan pengawasan tanpa sepengetahuan pengguna.

5. Kesimpulan

   Aplikasi FlexiSpy dibuat untuk mengawas karyawan, tetapi aplikasi ini sejati nya adalah aplikasi pengintai yang dapat disalahgunakan oleh orang lain

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