Laporan Aktifitas Malware : ShadySpy

Tanggal : 02 Oktober 2024

Waktu Mulai : 14.30 WIB

Waktu Selesai : 15.00 WIB

Nama Malware : ShadySpy

Jenis Analisis : Statis

1. Deskripsi Malware

   ShadySpy merupakan spyware yang ditujukan untuk orang tua memantau isi ponsel 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.shadyspy.monitor
      - Waktu mulai : 14.33 WIB
      - Aktivitas : meminta perizinan pengguna

   b. Koneksi Jaringan
      - Domain terhubung : shadyspy.com
      - Ip address : 45.79.149.154
      - Tipe koneksi : TCP

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

   d. Persetujuan yang mencurigakan
      - android.permission.REQUEST_INSTALL_PACKAGES,
      - android.permission.FOREGROUND_SERVICE,
      - com.google.android.c2dm.permission.RECEIVE,
      - com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

4. Analisis Perilaku

   Pengamatan : ShadySpy akan meminta perizinan pengguna untuk akses direktori, catatan telepon, sms, notifikasi, dan Lokasi detail. Lalu aplikasi akan menghapus icon/shortcut aplikasi nya

   Tindakan berbahaya : ShadySpy dapat menjadi aplikasi berbahaya jika digunakan oleh pihak yang tidak bertanggung jawab atau disalah gunakan

5. Kesimpulan

   ShadySpy merupakan aplikasi untuk memfasilitasi orang tua untuk memantau kegiatan anak mereka, tapi aplikasi ini memiliki fitur yang dapat digunakan untuk orang memata-matai orang lain

6. Rekomendasi

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