Laporan Aktifitas Malware : snoopza

Tanggal : 26 September 2024

Waktu Mulai : 17.09

Waktu Selesai : 17.30

Nama Malware : snoopza

Jenis Analisis : Statis

1. Deskripsi Malware

   Snoopza adalah aplikasi pemantauan ponsel yang memungkinkan pengguna untuk melacak berbagai aspek perangkat target.

2. Metodologi

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

3. Aktivitas yang ditemukan
   a. Proses yang dijalankan
      - Proses utama : setup-325n8.apk
      - Waktu mulai : 17.10
      - Aktivitas : meminta perizinan pengguna

   b. Koneksi Jaringan
      - Domain terhubung : i2.ytimg.com
      - Ip address : 64.233.170.102
      - Tipe koneksi : TCP

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

- android.permission.WRITE_SETTINGS,
- android.permission.SYSTEM_ALERT_WINDOW

d. Persetujuan yang mencurigakan
- android.permission.ACCESS_BACKGROUND_LOCATION,
- android.permission.READ_CALENDAR,
- android.permission.PROCESS_OUTGOING_CALLS,
- android.permission.PACKAGE_USAGE_STATS,
- android.permission.BLUETOOTH,
- android.permission.MODIFY_AUDIO_SETTINGS,
- android.permission.REQUEST_INSTALL_PACKAGES,
- android.permission.FOREGROUND_SERVICE,
- android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS

4. Analisis Perilaku

Pengamatan : Aplikasi pertama kali akan menginstall *agent* yang berfungsi untuk komunikasi dengan server dan mulai mendownload script-script essential

Tindakan berbahaya : aplikasi snoopza dapat digunakan untuk memata-matai seseorang, mengumpulkan berbagai data sensitif dan dapat di unduh secara luring

5. Kesimpulan

Aplikasi Snoppza merupakan aplikasi pemantau yang dapat digunakan oleh peretas jahat untuk menyusup lalu mendapatkan hak akses penuh ke korban dan mencuri informasi sensitive

6. Rekomendasi
   a. Jika ditemukan pada perangkat, segera lakukan pemindaian dengan perangkat lunak anti-malware atau anti-spyware untuk mendeteksi dan menghapus spyware ini.
   b. Aktifkan autentikasi dua faktor (2FA) dan gunakan kata sandi yang kuat untuk mencegah akses tidak sah.