Laporan Aktifitas Malware : TheTruthSpy

Tanggal : 26 September 2024

Waktu Mulai : 09.00 WIB

Waktu Selesai : 09.15 WIB

Nama Malware : TheTruth Spy

Jenis Analisis : Statis

1. Deskripsi Malware

   TheTruthSpy merupakan aplikasi pemantauan handphone, pengguna diwajibkan membaca dan mengerti Syarat dan Ketentuan penggunaan aplikasi TheTruthSpy sehingga aplikasi ini menjadikan tanggung jawab pengguna sepenuh nya dan pihak pengembang tidak menanggung akibat yang ditimbulkan oleh pengguna

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.systemservice
      - Waktu mulai : 09.00
      - Aktivitas : menciptakan *hash* sha256

   b. Koneksi Jaringan
      - Domain terhubung : protocol-a.thetruthspy.com, thetruthspy.com
      - Ip address : 154.12.231.82, 172.67.174.162
      - Tipe koneksi : TCP

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

- android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED

d. persetujuan yang mencurigakan
   - android.permission.FLASHLIGHT, android.permission.READ_CALENDAR, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.MODIFY_AUDIO_SETTINGS,
   - android.permission.PROCESS_OUTGOING_CALLS, android.permission.CALL_PHONE, android.permission.CHANGE_WIFI_STATE, android.permission.CHANGE_NETWORK_STATE,
   - android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.ACCESS_SUPERUSER, android.permission.FOREGROUND_SERVICE,
   - com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID

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 TheTruthSpy dapat digunakan untuk menguntit orang yang tidak mengerti tentang teknologi, bahkan dapat mencari informasi sensitif di dalam handphone pengguna

5. Kesimpulan

   Aplikasi TheTruthSpy 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 TheTruthSpy
   b. Segera ganti semua password/akses masuk dan terapkan 2MFA

Lampiran :

1 (Satu) file aplikasi TheTruthSpy

TheTruthSpy.apk