Laporan Aktifitas Malware : Mrecorder

Tanggal : 02 Oktober 2024

Waktu Mulai : 14.05 WIB

Waktu Selesai : 14.30 WIB

Nama Malware : Mrecorder

Jenis Analisis : Statis

1. Deskripsi Malware

   Mrecorder merupakan aplikasi pemantau yang cukup lama/jadul dan sudah masuk kedalam database play protect
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.mobileservices2.synchronization
      - Waktu mulai : 14.06 WIB
      - Aktivitas : Meminta pengguna untuk menonaktifkan fitur “play protect”

   b. Koneksi Jaringan
      - Domain terhubung : instructions.mobilerecorder24.com, dispatcher.mrecorder.com
      - Ip address : 108.138.141.85, 18.67.175.103
      - Tipe koneksi : TCP

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

   d. Persetujuan yang mencurigakan
      - android.permission.CHANGE_WIFI_STATE,
      - android.permission.CHANGE_NETWORK_STATE,
      - android.permission.PROCESS_OUTGOING_CALLS,

- android.permission.FOREGROUND_SERVICE,
- android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS,
- com.google.android.c2dm.permission.RECEIVE,
- com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

4. Analisis Perilaku

   Pengamatan : Mrecorder merupakan spyware yang tergolong cukup lama, dan tidak mendukung semua versi android. Aplikasi ini akan langsung terdeteksi jika play protect tidak dimatikan

   Tindakan berbahaya : Mrecorder berbahaya jika berhasil di install tanpa ada nya intrusi dari play protect

5. Kesimpulan

   Mrecorder merupakan spyware yang cukup lama dan sudah tercatat dalam database play protect sebagai ‘virus’. Jangan pernah matikan fitur play protect pada handphone android

6. Rekomendasi

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