Laporan Aktifitas Malware : Spymie

Tanggal : 30 September 2024

Waktu Mulai : 10.59 WIB

Waktu Selesai : 11.17 WIB

Nama Malware : Spymie

Jenis Analisis : Statis

1. Deskripsi Malware

   Spymie merupakan spyware berjenis keylogger yang bertujuan untuk merekam sentuhan layer pengguna dan juga input dari user juga, seperti text dan sentuhan layer

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.ant.spymie.keylogger
      - Waktu mulai : 10.59 WIB
      - Aktivitas : meminta perizinan pengguna

   b. Koneksi Jaringan
      - Domain terhubung : play.google.com
      - Ip address : 74.125.24.101
      - Tipe koneksi : TCP

   c. Persetujuan yang biasanya ada di malware
      - android.permission.ACCESS_NETWORK_STATE,
      - android.permission.INTERNET

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

4. Analisis Perilaku

   Pengamatan : Spymie akan meminta perizinan seperti internet, gps, penyimpanan untuk melengkapi fitur applikasi tersebut, lalu mulai menghubungi server penerima

   Tindakan berbahaya : Spymie dapat menyimpan log/catatan apa saja yang pengguna pernah ketik/sentuh lalu mengirim ke server penerima

5. Kesimpulan
   Spymie merupakan aplikasi keylogger yang bertujuan untuk menyimpan catatan/log pengguna lalu mengirim ke server penerima, aplikasi ini sangat berbahaya karena tidak dapat di lihat prosesnya dan sangat minim gangguan bagi pengguna sehingga pengguna merasa tidak ada yang aneh pada handphone nya

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