Laporan Aktifitas Malware : Appmia

Tanggal : 01 Oktober 2024

Waktu Mulai : 13.24 WIB

Waktu Selesai : 13.50 WIB

Nama Malware : Appmia

Jenis Analisis : Statis

1. Deskripsi Malware
   Appmia merupakan spyware yang dibuat dengan tujuan untuk memata-matai seseorang

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.polisoutgel.appmiorefe
      - Waktu mulai : 13.25
      - Aktivitas : meminta perizinan user dan mengecek status root

   b. Koneksi Jaringan
      - Domain terhubung : d1byvlfiet2h9q.cloudfront.net, daneden.me
      - Ip address : 18.64.22.32, 76.76.21.123
      - Tipe koneksi : TCP

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

   d. Persetujuan yang mencurigakan

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

5. Kesimpulan
   Aplikasi Appmia merupakan aplikasi yang memang dibuat dengan tujuan memata-matai seseorang, terlihat dari nama aplikasi yang tidak mencurigakan

6. Rekomendasi
   a. Segera hapus jika pengguna tidak sadar menginstall aplikasi Appmia
   b. Segera ganti semua password/akses masuk dan terapkan 2MFA