Laporan Aktifitas Malware : Xhunter

Tanggal : 02 Oktober 2024

Waktu Mulai : 16.45 WIB

Waktu Selesai : 17.03 WIB

Nama Malware : Xhunter

Jenis Analisis : Statis

1. Deskripsi Malware

   Xhunter merupakan spyware yang ditujukan untuk kegiatan pembelajaran malware saja, tetapi banyak orang yang memanfaatkan Xhunter untuk kepentingan pribadi

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.xhunter
      - Waktu mulai : 16.49 WIB
      - Aktivitas : membuat database di penyimpanan internal

   b. Koneksi Jaringan
      - Domain terhubung : -
      - Ip address : -
      - Tipe koneksi : -

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

   d. Persetujuan yang mencurigakan
      - -

4. Analisis Perilaku

   Pengamatan : Xhunter merupakan aplikasi ‘builder’ yang tujuannya adalah membuat aplikasi jahat baru dengan koneksi jaringan yang ditargetkan ke server penerima

   Tindakan jahat : Xhunter dapat disalahgunakan untuk mencuri data orang lain

5. Kesimpulan

   Xhunter merupakan aplikasi jahat yang dapat digunakan untuk media pembelajaran, tapi kemungkinan terbesar adalah untuk kepentingan pribadi

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