Laporan Aktivitas Malware: Pegasus Spyware
Tanggal: 03 Oktober 2024
Waktu Mulai: 12.30 WIB
Waktu Selesai: 12.58 WIB
Nama Malware: Pegasus Spyware
Tools analisis : Mobsf

1. Deskripsi Malware

Pegasus adalah perangkat lunak mata-mata *(spyware)* yang dikembangkan oleh NSO Group, perusahaan keamanan siber dari israel. Spyware ini tidak bisa terdeteksi dengan mudah pada perangkat yang telah disusupi. *Pegasus* memiliki kemampuan yang sangat canggih, termasuk kemampuan untuk merekam panggilan, membaca pesan teks, menyusup ke aplikasi pesan instan, memotret melalui kamera, dan merekam aktivitas pengguna lainnya.

2. Metodologi

Analisis dilakukan di lingkungan Mobsf dengan static analysis di mobsf.

3. Aktivitas yang Ditemukan

a. Proses yang Dijalankan
Proses Utama: Pegasus.apk
Waktu Aktivasi: 12.30 WIB.
b. Koneksi Jaringan
Country : Israel
IP Address: -
Port: -
Tipe Koneksi: -
Waktu Koneksi: 12.30 WIB

4. Behavior Analysis

Malware ini mampu merekam, memotret, menyusup ke pesan instan, melacak nomor dan lokasi device

5. Kesimpulan

Pegasus Spyware adalah spyware yang dikembangkan untuk keperluan militer dan menjadi ancaman keamanan siber

6. Rekomendasi

- Pasang antivirus pada perangkat anda
- Berhati hati dalam mengklik sebuah tautan