

## Laporan Aktifitas Malware : CatWatchFul

Tanggal : 30 September 2024

Waktu Mulai : 09.37 WIB

Waktu Selesai : 09.50 WIB

Nama Malware : CatWatchFul

Jenis Analisis : Statis

### 1. Deskripsi Malware

CatWatchFul merupakan spyware yang dijadikan sebuah service oleh organisasi CatWathFul untuk memantau handphone karyawan

### 2. Metodologi

Analisis dilakukan dengan metode static yang di operasikan menggunakan MobSF Static Analyzer

### 3. Aktivitas yang ditemukan

#### a. Proses yang dijalankan

- Proses utama : cwf\_installer.apk
- Waktu mulai : 09.37 WIB
- Aktivitas : Meminta perizinan pengguna

#### b. Koneksi Jaringan

- Domain terhubung : catwatchful.pink
- Ip address : 69.48.143.14
- Tipe koneksi : TCP

#### c. Persetujuan yang biasanya ada di malware

- android.permission.INTERNET,
- android.permission.WRITE\_EXTERNAL\_STORAGE

#### d. Persetujuan yang mencurigakan

- android.permission.REQUEST\_INSTALL\_PACKAGES

### 4. Analisis Perilaku

Pengamatan : CatWatchFul akan meminta perizinan untuk akses direktori, lalu akan meminta perizinan untuk menginstall aplikasi dari sumber yang tidak terpercaya/pihak ketiga

Tindakan berbahaya : aplikasi CatWathFul akan menginstall aplikasi 'persistent' nya dan akan sulit dideteksi oleh pengguna

5. Kesimpulan

Aplikasi CatWathFul merupakan aplikasi spyware yang tujuan utamanya adalah memantau kegiatan/aktivitas karyawan secara diam-diam, aplikasi ini dapat memantau bahkan sampai mengendalikan handphone secara remote/diam-diam

6. Rekomendasi

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