

Laporan Aktifitas Malware : Screen Time Parental Control

Tanggal : 04 Oktober 2024

Waktu Mulai : 10.04 WIB

Waktu Selesai : 10.35 WIB

Nama Malware : Screen Time Parental Control

Jenis Analisis : Statis

1. Deskripsi Malware

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.screentime
- Waktu mulai : 10.05
- Aktivitas : meminta perizinan pengguna

b. Koneksi Jaringan

- Domain terhubung : screentimelabs.com
- Ip address : 141.193.213.20
- Tipe koneksi : TCP

c. Persetujuan yang biasanya ada di malware

- android.permission.WRITE_SETTINGS, android.permission.READ_SMS,
- android.permission.RECEIVE_SMS, android.permission.READ_PHONE_STATE,
- android.permission.READ_CONTACTS, android.permission.READ_CALL_LOG,
- android.permission.INTERNET,
- android.permission.ACCESS_NETWORK_STATE,
- android.permission.RECEIVE_BOOT_COMPLETED,
- android.permission.GET_TASKS,
- android.permission.SYSTEM_ALERT_WINDOW,
- android.permission.ACCESS_FINE_LOCATION,
- android.permission.ACCESS_COARSE_LOCATION,
- android.permission.WAKE_LOCK,
- android.permission.READ_EXTERNAL_STORAGE,
- android.permission.WRITE_EXTERNAL_STORAGE

d. Persetujuan yang mencurigakan

- com.google.android.c2dm.permission.RECEIVE,

- android.permission.REQUEST_INSTALL_PACKAGES,
- android.permission.PACKAGE_USAGE_STATS,
- android.permission.ACCESS_BACKGROUND_LOCATION,
- android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS,
- android.permission.FOREGROUND_SERVICE,
- com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE,
- com.google.android.gms.permission.AD_ID

4. Analisis Perilaku

Pengamatan : Screen Time Parental Control akan meminta perizinan pengguna seperti jaringan dan gps untuk memantau lokasi akurat handphone anak mereka berada.

Tindakan berbahaya : aplikasi ini memiliki fitur persistent yang sulit untuk di hapus

5. Kesimpulan

Screen Time Parental Control merupakan malware yang tujuan utamanya untuk orang tua mengawasi handphone anak mereka

6. Rekomendasi

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