Trojan and Spyware Incident Report: Alleged Involvement of Ashley [redacted] in the Compromise of the Client's and their Son's Device (Owned by the Client) - Samsung A03s Device

---

Executive Summary

This report presents the results of an in-depth penetration test and vulnerability assessment on the **Hiya/Service** application and associated components on a **Samsung A03s device**. The investigation revealed the presence of malicious software, including a Trojan, SQL injection vulnerabilities, and spyware, embedded in an unofficial application. The findings suggest a high likelihood that **Ashley** [redacted] who previously held parental control over the device, was involved in the installation or facilitation of these threats.

Her role as the parental control administrator raises serious concerns about the abuse of privileges, leading to unauthorized data collection, privacy breaches, and security risks for her son.

Scope of Assessment

- **Target Application**: Hiya/Service (Version 12, Build 31)
- **Additional Components**: Google Partner Setup (Version 100.448391512)
- **Potential Malicious Application**: air.com.playtika.sfotomania
- **Suspect**: [redacted]

Detailed Findings

Application Overview: Hiya/Service

- **Version**: 12
- **Build Version**: 31
- **Permissions**: Requests sensitive permissions, including RECEIVE_BOOT_COMPLETED and READ, along with other elevated custom permissions.
- **Special Access**: Extensive privileges, including full network access and the ability to modify system settings.

Trojan Detection

Malicious APK Identified:

- **Package Name**: air.com.playtika.sfotomania
- **MD5 Hash**: e7e4810f0c7c6a109d5bc0b309beecac
- **SHA256 Hash**: fab1460dd30fa04568eb935a1fddfec93535031c54f8d5e0d4046d42af7c8f6b

Analysis Results:

Static and behavioural analysis flagged this APK as a Trojan, displaying unauthorized data access, network communications consistent with known Trojan activity, and patterns typical of command-and-control (C2) systems.

SQL Injection Vulnerability