FLY

Защищенный телефон

Техническое описание

ОБЩАЯ ИНФОРМАЦИЯ

Программный продукт AVSOFT FLY обеспечивает конфиденциальность коммуникаций, безопасность и маскировку данных пользователя.

AVSOFT FLY разработан на базе ОС Android 15 и позволяет управлять и контролировать функции, программное обеспечение и оборудование смартфона.

ОСНОВНЫЕ ФУНКЦИИ

1. Отсутствие программных закладок и утечек со стороны ОС

• прошивка основана на ОС с открытым кодом LineageOS на базе Android 15 версии, без внедрённых проприетарных сервисов (в т.ч. GMS, OTA-сервисов, аналитики)

• исключены встроенные компоненты телеметрии, используемые большинством производителей

• исходный код прошивки открытый, доступен для аудита и модификации

2. Изменение идентификаторов мобильного устройства и ОС

• подмена параметров идёт в связке для соответствия определённым профилям пользователей

• профили подготавливаются заранее с возможностью оперативного переключения

• возможность подмены идентификаторов мобильного устройства и ОС: название устройства, производитель, кодовое название устройства, версия Android, отпечаток устройства), смена MAC-адреса Wi-Fi адаптера, связки данных eSIM+IMEI+s/n+MEID

• смена всех идентификаторов происходит с автоматическим переключением в авиарежим с целью маскировки проводимых действий со стороны операторов сотовой связи

3. Изменение геолокации и показаний сенсоров

• подмена GPS-координат на уровне приложений

• подмена показаний: акселерометра, гироскопа, компаса, датчика освещённости.

4. Контроль за аппаратными модулями телефона

• полный запрет на использование камеры, микрофона, Wi-Fi, Bluetooth, NFC, сканера отпечатков на уровне приложений препятствует их включению стандартными средствами

• возможность сохранения изображения с камеры в защищённое хранилище, без сохранения его в стандартном альбоме

5. Настраиваемые политики доступа для приложений

• полный запрет приложениям на доступ в интернет

• запрет на доступ к информации об установленных приложениях

• скрытие контактов

6. Блокировка установки приложений и использования USB

• запрет установки APK из любых источников

• запрет на удаления приложений

• ограничение доступа через USB с возможностью использования подключения только заряда телефона (запрет отладки)

7. Подмена пользовательских данных

• подмена по заранее подготовленным профилям (была ошибка в слове) данных в связке: телефонная книга, входящие/исходящие вызовы, sms с автоматической установкой актуальных дат.

• реализация скрытия отдельных контактов для выбранных приложений

8. Защита интернет-трафика и контроль сетевой активности

• использование TOR приложения, собранного из проекта с открытым кодом

• использование защищённого браузера на основе проекта с открытым кодом:

- блокировка рекламы, трекеров, файлов cookies, цифровых отпечатков
- защита от вредоносного ПО, фишинга и междоменного отслеживания
- выбор клиента браузера (телефон/ПК)

• выход в интернет может быть ограничен явно заданными маршрутами и доверенными узлами проксирование на уровне ОС (iptables)

9. Прочее

• предупреждение в виде уведомления о вводе запрещённой последовательности символов с целью недопущения ввода пользователем реальных данных (ФИО, номер телефона, номер банковской карты, прочие слова и словосочетания из справочника)

• сигнализация о возможном подключении к виртуальной базовой станции (ВБС)

• защищённое файловое хранилище

• запрет на добавление сторонней клавиатуры

• сброс данных телефона при 5 неправильных вводах пароля

МЕХАНИЗМЫ ЗАЩИТЫ

- Кибербезопасность
- Подмена данных
- Защищённое хранилище
- Анти-MITM
- Удаленное управление устройством
- Мгновенное скрытие фотографий при фотосъёмке

ЗАЩИТА ДАННЫХ

Сообщения	Камера	Сведения о параметрах телефона и ОС
Звонки	Микрофон	
Контакты	Показания датчиков	

ПРЕИМУЩЕСТВА

- Контроль доступа к данным со стороны приложений и служб ОС
- Защита данных на уровне операционной системы (контролируемая прошивка)
- Программный контроль работы аппаратной составляющей телефона (камера, микрофон, датчики геопозиции и т.д.)
- Прошивка полностью контролируется и не использует встроенные сервисы Google. Обеспечивает защиту от шпионажа и утечки данных. Возможна интеграция в корпоративные DLP-решения.
- Отсутствие зависимости от Google Services, что защищает телефон от отправки информации на сервера Google, повышает скорость загрузки устройства и увеличивает срок его работы на одном заряде