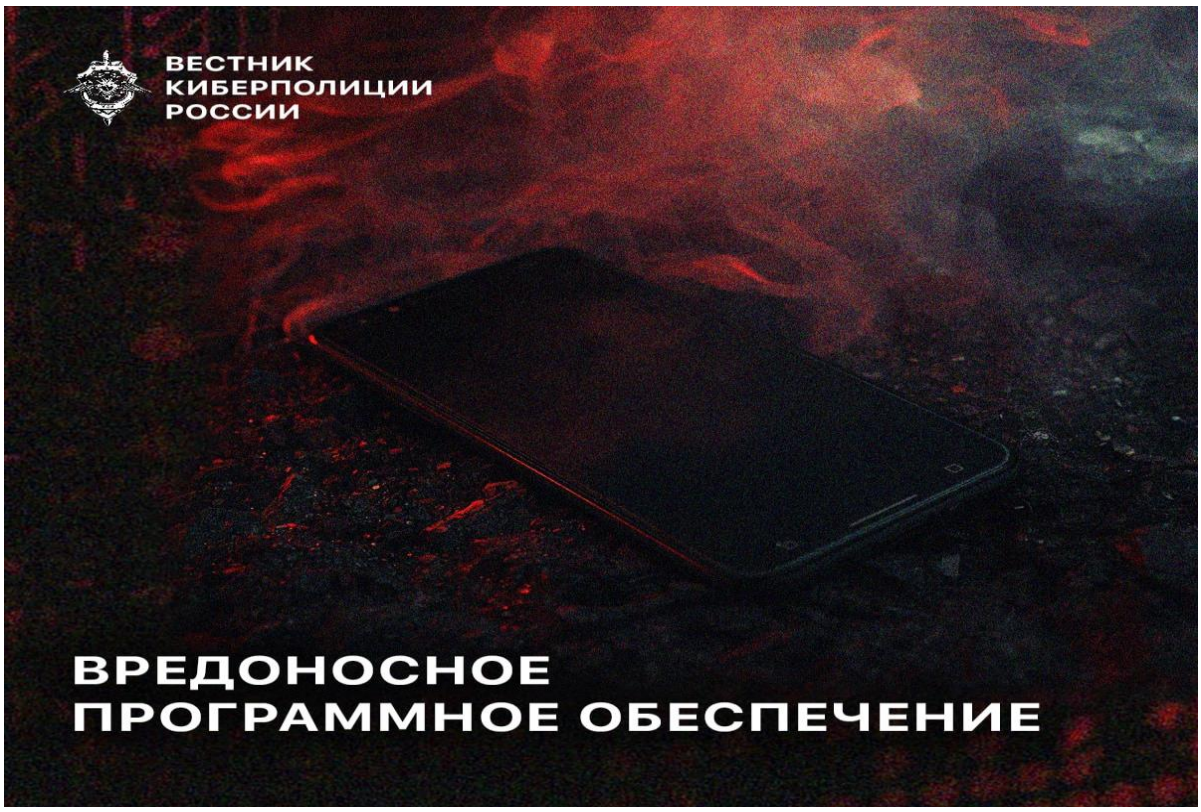

Ранее мы уже рассказывали о распространённых вредоносных программах, активно используемых в мошеннических схемах в России: банковском трояне Mamont, модификации NFCGate и RAT-утилите CraxsRAT.

Арсенал киберпреступников постоянно пополняется - нами зафиксирован рост активности шпионских программ LunaSpy и SpyNote.

LunaSpy — программа шпион, распространяется через мессенджеры под видом антивируса и программ банковских защитников.

Функции:

- Имитирует сканирование и показывает фальшивые угрозы.
- Перехватывает сохранённые пароли из браузеров, записывает экран, крадёт галерею.
- Записывает звук и видео с микрофона и камеры.
- Читает SMS, журнал звонков и список контактов.
- Запускает произвольные shell-команды.
- Отслеживает геолокацию.
- Записывает экран.

SpyNote — RAT (троян удалённого доступа). Используется телефонными мошенниками после «разговора поддержки» с просьбой установить «спецпрограмму для защиты».

Функции:

- Полный удалённый контроль над устройством,

- Перехват SMS и уведомлений,
- Overlay-атаки на банковские приложения.

Цель – получение доступа к онлайн-банкингу и мессенджерам.

Чтобы избежать заражения шпионскими программами вроде LunaSpy и SpyNote, устанавливайте приложения только из официальных магазинов, регулярно обновляйте систему и программы, ограничивайте права приложений и пользуйтесь надежными антивирусами. Не переходите по подозрительным ссылкам и файлам из мессенджеров, включите двухфакторную аутентификацию и будьте внимательны к рекламным баннерам и всплывающим окнам. Следование этим мерам существенно повысит вашу защиту.