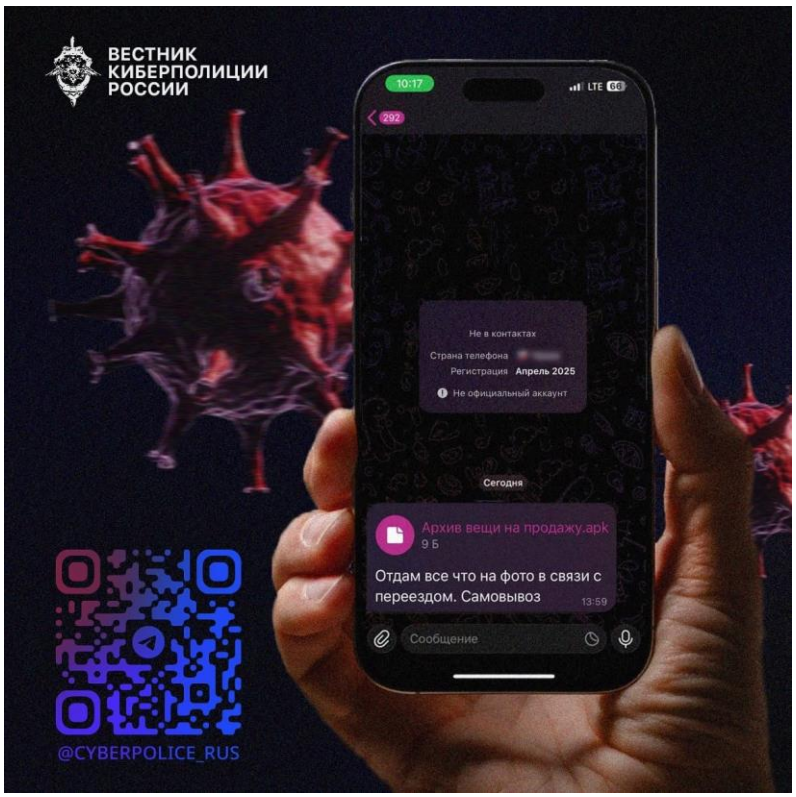

Старая схема, но в другой «упаковке»

Злоумышленники распространяют APK-файлы с названиями вроде «Фото 24шт.apk», выдавая их за архивы изображений. Суть не изменилась: под видом чего-то безобидного и срочного заинтересовать пользователя и спровоцировать установку вредоносного APK.

Такие файлы содержат вредоносное ПО семейства Mamont, предназначенное для скрытого сбора данных и удалённого управления устройством.

Что делает вредонос:

🔻Запрашивает доступ к SMS, контактам, звонкам и камере
🔻Запускается автоматически при включении устройства
🔻Может отправлять USSD-команды, читать и удалять SMS, открывать произвольные ссылки
🔻Передаёт данные о состоянии устройства на удалённые серверы

После установки пользователь видит фишинговую страницу, имитирующую, к примеру, сервис обмена изображениями, в некоторых случаях используются легитимные сайты, чтобы не вызвать подозрений.

Напоминаем:

➡️Не устанавливайте APK-файлы из чатов, мессенджеров и непроверенных источников
➡️Отключите автозагрузку файлов в Telegram
➡️Проверяйте подозрительные файлы через специальные сервисы
➡️Используйте антивирусное ПО на мобильных устройствах
➡️Не предоставляйте приложениям доступ к SMS, контактам и камере без явной необходимости

Будьте бдительны: даже «безобидный» на вид файл может скрывать угрозу, способную привести к утечке персональных данных и финансовым потерям.

✅Подписаться на Киберполицию России (t.me/cyberpolic...)