Полиция научилась обходить одну из главных защит iPhone: GrayKey сохраняет доступ даже после перезагрузки

Компания Magnet Forensics заявила, что ее инструменты GrayKey Preserve и Evidence Preservation Mode способны обходить функцию Inactivity Reboot в iPhone. Эта защита автоматически перезагружает смартфон после 72 часов без разблокировки и переводит его в более защищенное состояние BFU.

После первоначального доступа GrayKey, по данным утекшего обучающего видео, сохраняет состояние After First Unlock даже после перезагрузки или потери питания. Это делает часть данных доступнее для криминалистического анализа.

Инструмент также отключает сотовую связь, Wi-Fi и Bluetooth, чтобы изолировать устройство и не допустить удаленного изменения данных. Дополнительно система якобы способна сохранять кешированные геоданные, недавно удаленные фото и сообщения iMessage, которые обычно исчезают через определенное время.

Сама Apple внедрила Inactivity Reboot в iOS 18.1. После автоматической перезагрузки ключи шифрования для части данных становятся недоступны до первого ввода пароля, что заметно усложняет работу криминалистических инструментов.

Эксперт по безопасности iPhone Джиска Классен предположила, что GrayKey может манипулировать системными таймерами или отключать процессы, отвечающие за истечение срока хранения данных.

Технические детали обхода пока не опубликованы, а Apple и Magnet Forensics публичных комментариев не дали. Поэтому пока речь идет о заявленной возможности, а не о независимо подтвержденном взломе механизма защиты.

Григорьев С.М.
кандидат военных наук, доцент,
доцент кафедры «Безопасность жизнедеятельности»
Финансового университета при Правительстве РФ