Силовики прибегнут к “магии” при взломе Telegram

На днях во многих СМИ появилась информация о том, что в арсенале Следственного Комитета РФ появилось устройство, способное взломать любой смартфон и расшифровать переписку любого из популярных ныне мессенджеров. Официальное подтверждение этой информации можно найти на портале госзакупок. В документе утверждается, что СК в Центральном и Восточном военных округах на сумму в 5 миллионов рублей закупили у некой "ЭкспертЭкспресс" комплексы iDC-8811 Forensic MagiCube, созданные китайской компанией Xiamen Meiya Pico Information.



Судя по описанию устройства в контракте, оно действительно умеет многое, в том числе и расшифровывать переписку в популярных мессенджерах. Вот лишь немногие из возможностей доступных устройству согласно документу:

> *"3.23 Обнаружение в бинарном файле геолокационной информации, сохраняемой радиомодулями беспроводной связи, модулями GPS, а также ее декодирование в географические координаты.*
>
> *3.24 Обнаружение и декодирование истории сообщений, отправленных и полученных программными клиентами систем мгновенного обмена сообщениями (Skype, WhatsApp, Telegram, Viber, WeChat, Line).*
>
> *3.25 Обнаружение и декодирование пользовательской информации в программных клиентах социальных сетей.*
>
> *3.26 Возможность получения повышенных прав доступа к мобильным устройствам на базе ОС Android ("root") и для IOS ("jailbreak") в автоматическом режиме без использования программного обеспечения сторонних производителей.*
>
> *3.27 Возможность просмотра файлов на подключенном устройстве под управлением ОС Android при включенной отладке по USB.*
>
> *3.28 Физическое извлечение данных из мобильных устройств, основанных на процессорах Qualcomm, через сервисный коммуникационный порт 9008.*
>
> *3.29 Расшифровка и декодирование удаленной информации из образов памяти использованием технологии chip-off (чип-оф) из модулей памяти мобильных устройств Apple, Android".*

Также, согласно описанию во все том же документе, MagiCube подвластна и "магия" по взлому любого мобильного устройства, а если точнее, то порядка 3000 устройств ста компаний

производителей.

"MagiCube способен на физическое извлечение информации с возможностью обхода пользовательских кодов блокировки из мобильных устройств, построенных на базе процессоров Mediatek, Spreadtrum, Qualcomm", – говорится все том же документе.

Интересно, что на официальном сайте производителя устройства – компании MeyaPico – о столь грандиозных возможностях "магического куба" не говорится ни слова. MagiCube описывается как высокоинтегрированное компьютерное криминалистическое оборудование, предназначенное для работы с компьютерными и серверными жесткими дисками. Оно способно в кратчайшее время извлекать информацию с носителей, дублировать и анализировать ее.

Вот основные функции "магического куба", взятые с сайта производителя:

- Статическая и оперативная Криминалистика для автоматического анализа и создания отчетов в Mac OS X.
- ОС Windows и Linux.
- Анализ трассировки пользователя для доступа к журналам подключений USB-устройств, приложениям, последних открытых файлах, корзины и многое другое.
- Восстановление ключа реестра и журналов времени последнего изменения.
- Быстрый поиск и расположение анти-судебно-программного обеспечения и зашифрованных файлов.
- Настраиваемые стратегии судебной экспертизы для различных типов дел.

Как видно, ни о какой работе с мобильными устройствами не сказано ни слова. Так выглядит сие чудо:



[Силовики прибегнут к “магии” при взломе Telegram]

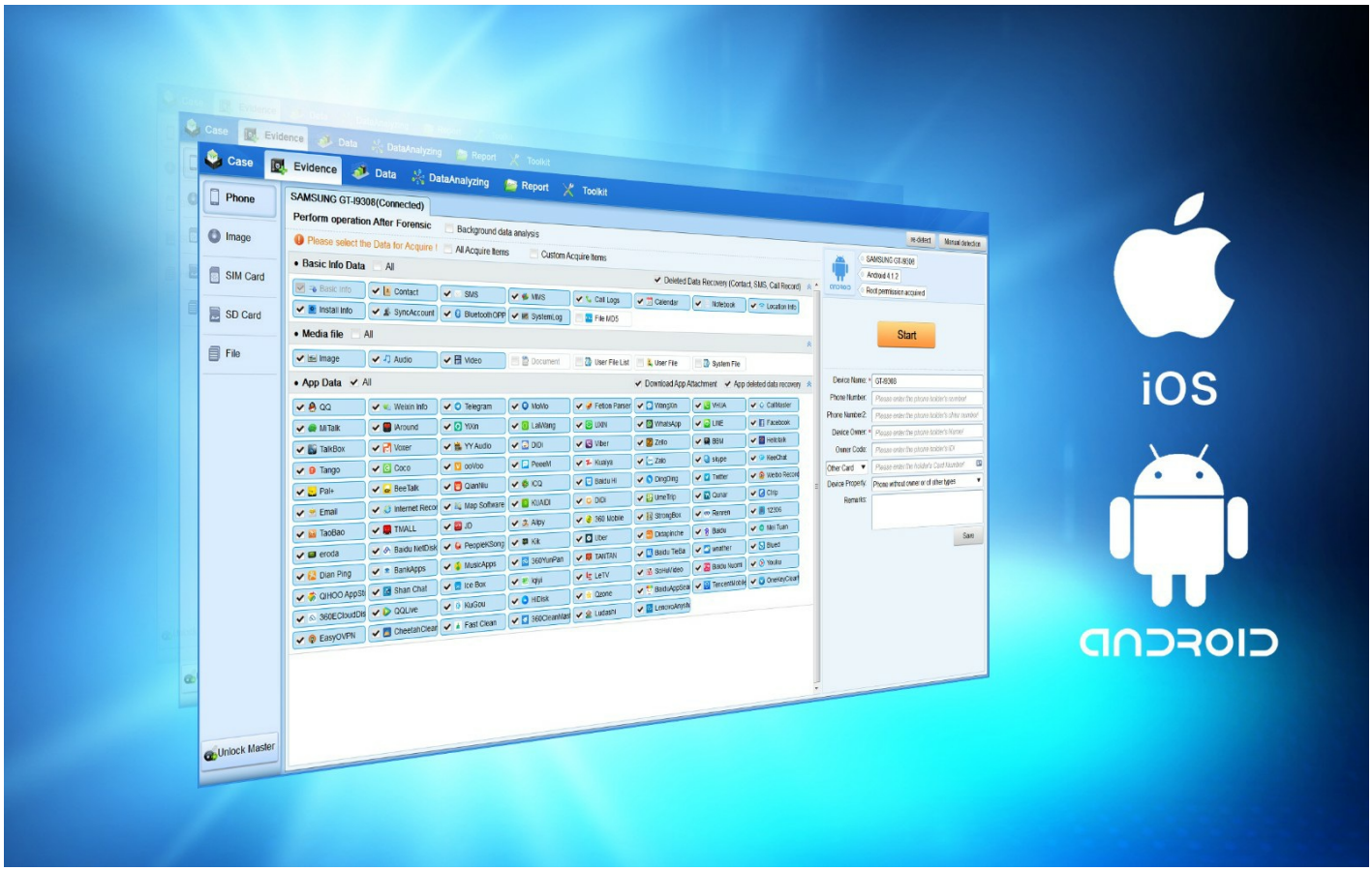
Вот видеоролик, наглядно демонстрирующий работу устройства:

Исходя из этого, можно усомниться в правдивости описания MagiCube в документе на портале Госзакупок. Однако, на самом деле вся сила "магического куба" в предустановленном программном обеспечении iDC-4501 Mobile Forensics System от все тех же MeyaPico. Как раз эта прошивка, по словам, производителя, и способна на взлом и расшифровку данных практически с любых мобильных устройств.

Например, согласно описанию, iDC-4501 Mobile Forensics System умеет:

- Извлекать и восстанавливать данные с мобильных устройств.
- С легкость взламывать ключи блокировки экрана, в особенности на мобильных устройствах китайских брендов.
- Способно извлечь информацию с iPhone с iOS 10 до iOS 11.1.2, а также практически из всех популярных приложений.

Вот несколько скриншотов "магического" ПО:



Android Unlock Master - Use to screen unlock or download flash image

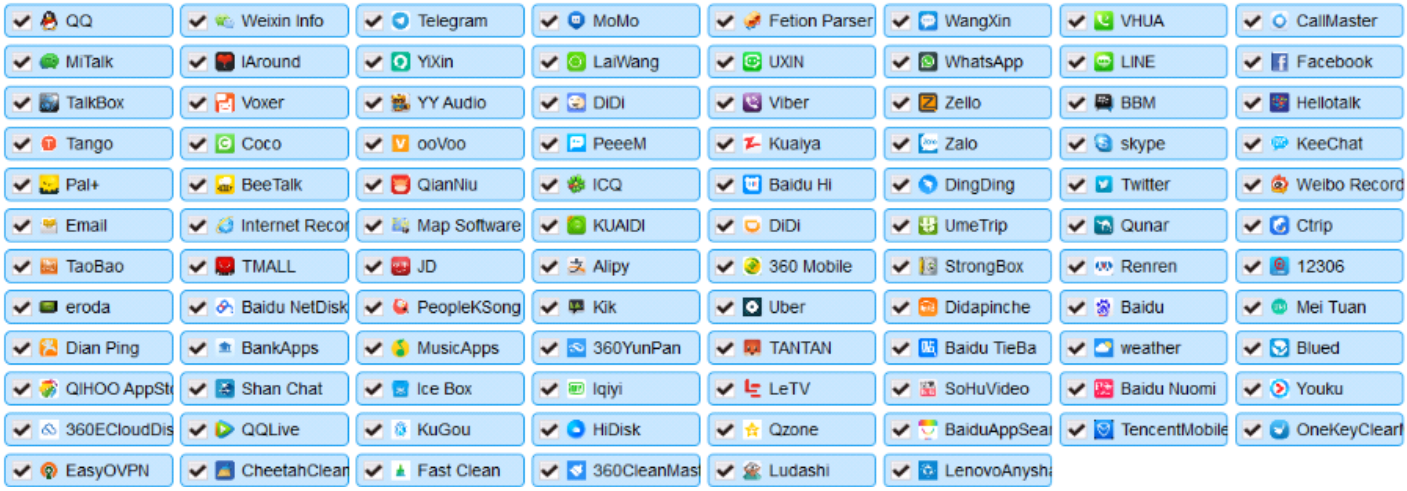
Home ▸ SAMSUNG

Back

The model on the back of Phone. Choose general model if target model not be found.

General model	SM-G9500 GALAXY S8	SM-G9550 GALAXY S8+	SM-G9350 GALAXY S7 Edge	SM-G9300 GALAXY S7
SM-G9308 GALAXY S7	SM-G930FD GALAXY S7	SM-G935FD GALAXY S7	GALAXY S7 Active	SM-G9250 GALAXY S6 Edge
SM-G9280 GALAXY S6 Edge+	SM-G9200 GALAXY S6	SM-G9208 GALAXY S6	SM-G9209 GALAXY S6	SM-G9006V GALAXY S5
SM-G9006W GALAXY S5	SM-G9008V GALAXY S5	SM-G9008W GALAXY S5	SM-G9009D GALAXY S5	SM-G9009W GALAXY S5
GALAXY S5 LTE-A	GALAXY S5 Mini	GALAXY S5 Neo	GALAXY S5 Sport	GT-I9500 GALAXY S4

Previous 1/10 Next



Впрочем, эксперты сильно сомневаются в возможностях MagiCube. Так, по словам Владимира Каталова, гендиректора компании Elcomsoft, ничего революционного MagiCube из себя не представляет:

> "MeyaPico - просто еще один разработчик среди примерно двух десятков, которые работают на этом рынке. Некие уникальные решения есть только у израильской компании Cellebrite. Самое интересное, что у них есть, - это софт Cellebrite, который массово закупает Следственный комитет, взламывая любые iPhone. Однако стоит учитывать, что израильской компании нужно физически получить сам смартфон, чтобы его "вскрыть". Понятно, что это тоже огромный риск, неизвестно, что они сделают с этим телефоном, помимо собственно взлома пароля и извлечения данных. Ведь никто не может проверить, сохраняют ли они эти данные себе или нет. Вторая компания, заслуживающая внимания, - это Greyshift. У них есть устройство для взлома пароля на iPhone, но они его продают с очень сильными ограничениями: только правоохранительным органам и только в Штатах и Канаде".

Смутили экспертов и утверждения о том, что MagiCube способен всего лишь за несколько минут взломать Iphone, в то время как известному израильскому производителю аналогичного оборудования на это нужно около суток.

> "Это какая-то пиар-история, которых, к сожалению, в области информационной безопасности становится все больше. К реальности она имеет весьма опосредованное отношение. Мы живем сейчас в мире пресс-релизов. До тех пор, пока мы не увидим хотя бы видеоролика, на котором виден процесс взлома смартфонов, верить этим историям просто невозможно. Тот, кто обладает эффективными инструментами в той или иной сфере, даже скорее не заинтересован, чтобы о таких возможностях кто-то что-то узнал, потому что все это прекрасно перекрывается, подлежит блокировке со стороны владельца операционной системы или разработчика смартфона", – рассказал "Коммерсанту" IT-эксперт Сергей Вильянов.

Эксперты подчеркивают, что силовым структурам стоит с осторожностью относиться к иностранному оборудованию такого класса. Ведь неизвестно куда могут уходить данные добываемые силовиками с устройств в ходе расследования.

В общем и целом, пока неясно будет ли реальная польза от "магического куба" из Китая, обошедшегося государству в несколько миллионов, и сможет ли он, как заявлено производителем, с легкость взламывать "айфоны" и расшифровывать переписку террористов в Telegram. Во всяком случае, экспертное сообщество относится к такой возможности с максимальным скепсисом.