

Текст · 3 июля 2023, 16:49

Ольга Ромашова,

Кто, где, когда. New York Times описала новую систему слежки за пользователями мессенджеров — насколько все плохо?

Газета *New York Times* выпустила статью, посвященную возможностям ранее малоизвестного инструмента для слежки за пользователями мессенджеров. Со ссылкой на внутренние документы издание описывает возможности программы *NetBeholder*, которую используют российские силовики. «Медиазона» поговорила с экспертами о возможностях этой системы и о способах избежать слежки или как минимум сильно усложнить ее.

Новый инструмент слежки для российских силовиков

Издание *New York Times* выпустило статью о возможностях цифровой слежки, которыми обладают российские власти. Журналисты получили «сотни файлов» от человека, который имел доступ к внутренним документам. Газета подробно описывает широкие возможности инструмента *NetBeholder* от компании *MFI Soft*, дочки *Citadel Group*, которую раньше частично контролировал Алишер Усманов.

В 2013 году в издании *Wired* описывалась программа с тем же названием — *NetBeholder*. На международном рынке ее представляла канадская

компания **ALOE Systems**, подразделение **MFI Soft**. Уже тогда в статье упоминались связи **MFI Soft** с Кремлем и спецслужбами. Автор статьи в **Wired**, создатель сайта **Agentura.ru** Андрей Солдатов подтвердил, что в статье **New York Times** речь идет о том же самом приложении.

Как утверждает газета, *NetBeholder* может отслеживать местоположение разных телефонов в течение дня. Если эти телефоны в какой-то момент оказались рядом, то, вероятно, их владельцы встретились. Благодаря геолокации силовики могут составить карту взаимоотношений^[1] разных пользователей.

Программа также может проверить, как часто два или более телефонов находятся рядом, и выяснить, что у человека несколько телефонов.

Кроме того, *NetBeholder* может определить, «когда кто-то отправляет файл или подключается к голосовой сети в зашифрованных приложениях, таких как *WhatsApp*, *Signal* или *Telegram*», утверждает издание. Силовики получают информацию, «кто с кем разговаривает, когда и где, а также прикреплен ли файл к сообщению». Содержание сообщений и звонков им недоступно.

Газета упоминает и другие программы, которые, например, преобразуют перехваченные телефонные разговоры в текст, собирают пароли, введенные на незашифрованных сайтах, идентифицируют анонимных пользователей и взламывают учетные записи. Эти возможности перехвата данных давно известны и использовались как хакерами, так и силовиками.

Эксперты призывают не паниковать и использовать VPN

«Сенсации в этом материале нет. Там описаны те способы получения информации, которые спецслужбы используют годами, а то и десятилетиями», — подчеркивают в проекте «Роскомсвобода». Операторы связи, которые сотрудничают с силовиками, могут «по характерным признакам трафика» установить факт переписки или голосовой связи между *IP*-адресами, но узнать содержание беседы в зашифрованном мессенджере они не способны. Чтобы сбить силовиков с толку, эксперты советуют использовать *VPN*.

Директор «Общества защиты интернета» и автор телеграм-канала «ЗаТелеком» Михаил Климарев говорит, что единственное новое в статье *New York Times* — это название программы *NetBeholder*. «Можно ли сопоставлять звонки и понимать, кто с кем общается? Теоретически описываемая модель возможна, но практически прямо тяжело. Я с трудом представляю такую информационную систему, которая смогла бы обрабатывать такое количество данных», — отмечает он.

В тексте *New York Times* не уточняется, о каком именно типе соединения идет речь, когда силовики могут узнать, «кто с кем разговаривает». Вероятно, речь идет о *peer-to-peer*^[2] соединении, когда пользователи соединяются напрямую, без участия серверов *Telegram* или *Signal*. Например, в *WhatsApp* так работают все звонки и отключить эту опцию нельзя.

В случае если звонки осуществляются через сервер мессенджера, слежку осуществить труднее, объясняет Климарев: «По пакету Яровой^[3] все факты подключения к интернету каждого конкретного пользователя записываются в специальную базу данных. Дальше мы у конкретного пользователя выбираем все обращения в телеграм с точным указанием времени. Как он дальше находит, с кем ты общался? Он берет такие же срезы по каждому пользователю, сравнивает и [ищет совпадения], чтобы в это же время другой пользователь точно так же получал какой-то коннект от телеграма. То есть они, например, звонили друг другу. Таким образом, мы можем действительно сопоставить [эти факты]. Но с другой стороны, у нас десятки миллионов пользователей и много операторов связи».

Массовую слежку за пользователями мессенджеров организовать сложно, проще следить за какими-то конкретными пользователями, но польза для силовиков сомнительна: «Вы узнаете, что Навальный общается с Волковым по телеграму. Что, вы не знали этого раньше? А с другой стороны, чтобы получить это знание, нужно 800 раз подпрыгнуть». Необходимо собрать терабайты данных и переработать их, чтобы получить не слишком ценную информацию, и все это слишком дорого, уточняет Климарев.

Журналист-расследователь Андрей Захаров обращает внимание, что *New York Times* ссылается в том числе на фрагменты маркетинговых презентаций компаний, которые создают программы для слежки: «Насколько оно реально работает? Сколько там затрат идет для анализа? Это же вычисления определенного рода. Не просто там кнопку нажал, а вот какие-то мощности

[нужны]. Я в презентации могу все что угодно написать, чтобы продать этот софт».

Редакторы: Дмитрий Трещанин, Давид Френкель

Обновлено в 20:55. Добавлена ссылка на *Wired*.

-
1. Эта возможность давно известна, в частности на нее «Медиазона» опиралась, создавая карту перемещений фигурантов дела об убийстве Немцова. Данные были получены следствием.
 2. При таком типе соединения абоненты отправляют данные друг другу напрямую, без посредников. С одной стороны, это безопаснее, так как исключает возможность прослушки со стороны самого мессенджера; с другой — оператор связи видит факт подключения и то, между какими IP-адресами оно происходит.
 3. «Пакет Яровой» — два федеральных закона, которые обязали операторов связи хранить весь интернет-трафик и усилили контроль силовиков за пользователями.