Текст · 26 апреля 2024, 19:42
Давид Френкель,

Телеграм позволяет перейти в браузерную версию без логина. Как этим могут воспользоваться силовики — и как от этого защититься

Несколько российских журналистов обнаружили у себя в *Telegram* чужие сессии — кто-то зашел в их аккаунты с веб-версии мессенджера. Они уверяют, что не пользовались *Telegram* через браузер. Это могло произойти из-за автологина: если из приложения *Telegram* на мобильном телефоне открыть ссылку *web.telegram.org*, вы попадете в свой аккаунт в окне браузера без каких-либо дополнительных проверок.

В самой функции автологина нет ничего страшного, но если ваш телефон попадет в руки злоумышленников или силовиков, такую сессию из браузера легко украсть — и тогда ваш аккаунт смогут читать в реальном времени.

«Медиазона» воспроизвела такой способ и рассказывает, как от него защититься.

О странных сессиях в *Telegram* у троих[1] российских журналистов рассказал сегодня в своем канале расследователь Андрей Захаров. По словам Захарова, с ним связались трое коллег, которые заметили у себя в телеграме подозрительные сессии. *IP*-адрес этих сессий не совпадал с реальным местоположением[2] журналистов.

Захаров предположил, что это может быть не взлом, а результат случайного автологина с мобильного телефона. В начале апреля *IT*-специалист Михаил Климарев писал, что у российских силовиков есть возможность использовать функцию автологина для того, чтобы получать доступ к аккаунту пользователя.

«Медиазона» повторила этот способ.

Как украсть веб-версию телеграма

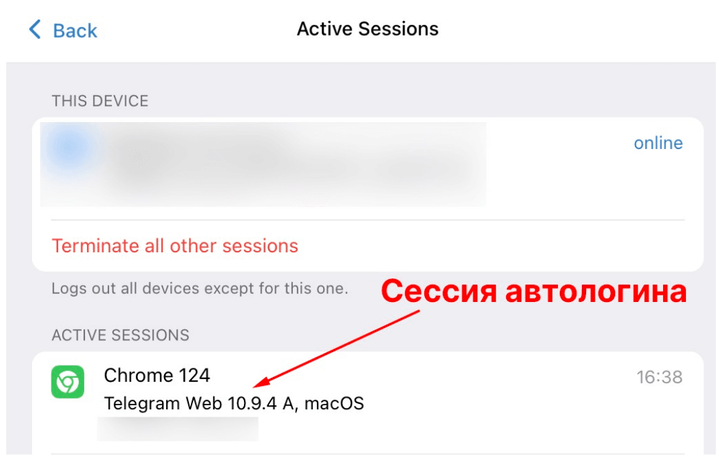
Чтобы зайти в тот же самый аккаунт с другого устройства, телеграм предлагает пользователю сфотографировать *QR*-код в том приложении, где у вас уже есть активная сессия, а потом ввести пароль.

> Кстати, если вы до сих пор не включили у себя в телеграме двухфакторную аутентификацию, сделайте это прямо сейчас. Это важно с точки зрения безопасности.

Этот процесс сильно упрощен в том случае, если вы решили зайти в веб-версию со своего мобильного телефона, где у вас уже установлено приложение.

Автологин в вашем браузере произойдет при любом нажатии на ссылку *web.telegram.org*[3] внутри мобильного приложения мессенджера. **То есть при нажатии на такую ссылку вы получите свой аккаунт в окне браузера без каких-либо дополнительных проверок (даже если включена двухфакторная аутентификация).**

Прямые ссылки на *web.telegram.org* можно встретить в каналах — авторы нередко вставляют их по ошибке. Мы предполагаем, что именно это и произошло с журналистами из поста Захарова: они нажали на ссылку, а телеграм автоматически их залогинил.



В самой такой функции нет ничего страшного, ведь вы и так имеете доступ к своему аккаунту на этом устройстве. Проблема в другом: эту сессию достаточно легко скопировать из браузера и получить таким образом доступ к веб-версии вашего аккаунта.

Такое может произойти, например, если при переходе российской границы вы разблокировали телефон и показали силовикам ваш телеграм, так как были уверены, что там нет ничего компрометирующего.

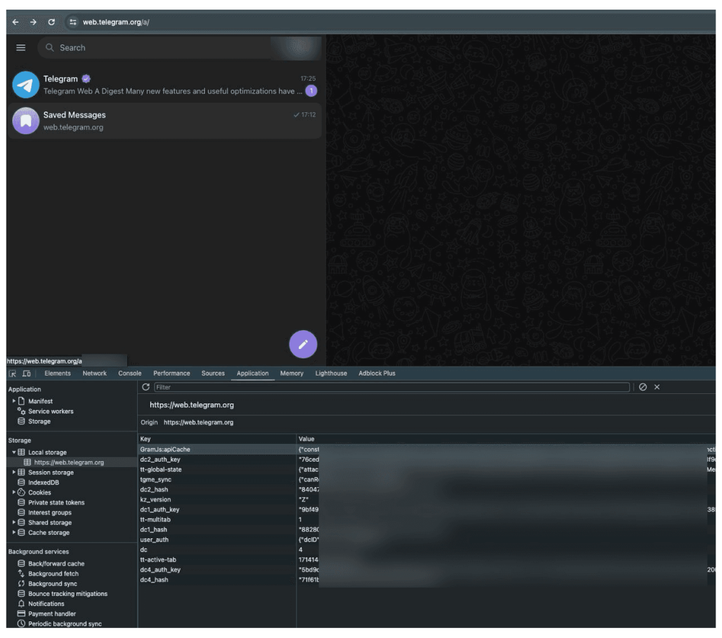
Силовики могут либо сами открыть веб-версию телеграма на вашем устройстве, либо скопировать уже готовую сессию из браузера — и таким образом получить постоянный доступ к вашему аккаунту до

тех пор, пока вы не почистите сессии. Это касается не только телеграма, но и вообще любых сайтов.

«Медиазона» смогла воспроизвести этот процесс. Мы создали новый аккаунт в телеграме с двухфакторной аутентификацией, в который зашли с *Android*-устройства (айфоны работают аналогично). Пройдя по ссылке, мы моментально получили доступ к тому же аккаунту в браузере *Chrome* этого же мобильного телефона. Никаких кодов или прохождения двухфакторной аутентификации не потребовалось.

Затем мы включили в настройках телефона опцию *USB Debugging* и подключили его к компьютеру. На компьютере, используя в браузере *Chrome* режим *Remote Debugger*, мы открыли вкладку с телеграмом, перешли в раздел, где хранятся сессии сайта в мобильном браузере, и полностью перенесли содержимое этого раздела в аналогичное место в браузер на компьютере.

После этого осталось лишь обновить до этого пустую страницу телеграма на компьютере, и мы получили полный доступ к тому же аккаунту, не проходя никаких дополнительных проверок, не зная никаких паролей или кодов. На других устройствах этот вход отображался как та же сессия, что была создана при автологине. После этого мы можем читать и копировать все новые переписки с этого аккаунта — до тех пор, пока пользователь принудительно не удалит эту сессию.



Большинство воспроизведенных нами действий несложно автоматизировать, так что таким методом за секунды можно собрать сессии ко всем популярным сайтам, не только к телеграму. Все, что для этого нужно силовикам, — ненадолго получить в свои руки разблокированный телефон (и для телеграма — войти в веб-версию с помощью автологина).

Если до этого вы не заходили в телеграм в браузере этого устройства, то сессия будет новой — вы получите уведомления о ней на других устройствах (если телефон — ваше единственное устройство, ничто не мешает силовикам скрыть уведомление). Но если вы уже делали так раньше (специально или по случайности), то никаких уведомлений об этом не будет, а в списке активных сессий не появится никаких новых: злоумышленник будет использовать вашу старую сессию.

> Судя по коду клиентов телеграма, который изучила «Медиазона», достать такую же сессию из самого приложения сложнее, например, в **Android**-клиенте сессии хранятся в специальном зашифрованном хранилище. Таким образом, автологин позволяет злоумышленникам получить доступ гораздо более простым путем чем через браузер, настолько простым, что это

удалось повторить корреспондентам «Медиазоны» самостоятельно.

Как от этого защититься

На момент публикации текста выключить автологин в мобильном приложении *Telegram* **нельзя**.

Если вы были вынуждены дать силовикам ваш разблокированный телефон, исходите из того, что их доступ к устройству позволяет сделать с ним все что угодно. К любым активным сессиям на этом устройстве мы рекомендуем относиться как к скомпрометированным.

Кроме того, стоит чаще проверять сессии в телеграме и в других приложениях и на сайтах; подозрительные нужно немедленно удалять и логиниться заново — особенно после того, как ваш телефон побывал в чужих руках. Постарайтесь вообще не сидеть в веб-версии телеграма.

Какие технологии есть у силовиков

В распоряжении российских силовиков есть целый набор средств, позволяющих им и взламывать смартфоны, и автоматизировать процесс съема информации с разблокированных устройств.

В 2021 году «Медиазона» выяснила, что во время расследования уголовного дела в отношении Любови Соболь ее телефоны пытались взломать при помощи устройств израильской компании *Cellebrite*, которую тогда официально поставляли

российскому Следственному комитету. Продукция компании — физические устройства, к которым можно подключить телефон, чтобы они при помощи известных уязвимостей в программном коде (или при разблокированном телефоне) сняли данные — от переписок до сохраненных фотографий.

Айфон и телефон *Xiaomi* Соболь, которую в итоге осудили по делу о проникновении в квартиру сотрудника ФСБ Константина Кудрявцева, предполагаемого участника отравления Алексея Навального, взломать не смогли, но сумели получить доступ к *iPhone 11 Pro* оператора Абдулкерима Абдулкеримова после «оперативно-розыскных мероприятий, направленных на установление пароля».

После публикации «Медиазоны» израильский юрист и правозащитник Эйтай Мак обратился в суд с требованием запретить *Cellebrite* продавать технологию в Россию. Компания, не дожидаясь рассмотрения иска, объявила о прекращении поставок в Россию и Беларусь.

Тем не менее уже после начала российского вторжения в Украину *Cellebrite* был успешно использован для доступа к телефону автора телеграм-канала «Протестный МГУ» Дмитрия Иванова, которого в итоге осудили по делу о распространении «фейков» об армии.

Альтернативой *Cellebrite* является российский комплекс «Мобильный криминалист», который прямо сообщает, что позволяет силовикам

использовать уязвимости в коде операционных систем для взлома айфонов и телефонов на *Android.*

---

1. На момент написания поста было известно о трех таких случаях, сейчас их четыре.
2. Двое находились в Германии, один — в России. При этом заход был из Швейцарии, другого города в Германии и из США.
3. Иногда открывается старая веб-версия “k” — возможно, если вы логинились в ней на этом устройстве. Однако ссылки вида web.telegram.org/a ведут только на новую версию и работают везде.