

15 сентября 2023 г.

РОССИЯ - ГЕРМАНИЯ

RSF требует тщательного расследования того, как Pegasus был использован для слежки за известной российской журналисткой в изгнании

Слежка за издательницей рижского независимого новостного сайта Meduza Галина Тимченко началась во время ее пребывания в Берлине. Глубоко потрясенные новым скандальным случаем наблюдения за журналистами при помощи шпионского программного обеспечения компании NSO, «Репортеры без границ» (RSF) призвали правительство Германии и все заинтересованные стороны провести быстрое и тщательное расследование.

В сообщении, опубликованном 13 сентября, независимыми лабораториями Access Now и Citizen Lab, сообщается, что шпионская программа Pegasus использовалась для слежки за российской журналисткой и издательницей независимого новостного сайта Meduza **Галиной Тимченко**. Согласно этому сообщению, смартфон Тимченко был заражен программой приблизительно 10 февраля 2023 года, в тот момент, когда она находилась на встрече в Берлине. Вплоть до момента проверки ее устройства в июне 2023 года ее безопасность и безопасность ее источников находилась под угрозой.

В этот период организация RSF организовала несколько встреч с находящимися в изгнании российскими журналистами и редакторами на которых обсуждались конфиденциальные и деликатные темы. Организация глубоко потрясена тем, что это может коснуться многих российских журналистов и, возможно, ее собственных сотрудников. Когда журналисты больше не могут, не опасаясь слежки, встречаться и обмениваться информацией, это напрямую влияет на их работу. Правительство Германии названо в [сообщении](#) в числе тех, кто может нести ответственность за слежку.

«Немецкие власти должны быстро отреагировать и провести тщательное расследование этого шокирующего случая. Он вызывает у RSF множество

животрепещущих вопросов, в частности: В какой степени правительство Германии было вовлечено в эту слежку и знало ли оно о них? Мы требуем немедленного и глубокого расследования фактов, а также строгих последствий для всех вовлеченных сторон».

Кристиан Мир,

Исполнительный директор RSF-Германия

Галина Тимченко основала независимое СМИ Meduza, находясь в изгнании в столице Латвии Риге. На сайте, который подвергается блокировке российскими властями и [разблокированном RSF](#), публикуются материалы на русском и английском языках. 26 января 2023 года, за две недели до заражения устройства Тимченко, это СМИ [было признано](#) в России «нежелательным», что означает, что любое сотрудничество с ним или его цитирование расценивается как преступление. В апреле 2022 года издание было объявлено в России «иностранным агентом». В том же году Тимченко была признана лучшим европейским журналистом года за неустанные усилия по обеспечению доступа населения России к независимой информации.

В своем сообщении Access Now и Citizen Lab перечислили три гипотезы о возможном происхождении хакерской атаки: согласно первой, основными подозреваемыми являются Германия, Эстония и Латвия; согласно второй – союзные России государства, такие как Азербайджан, Казахстан или Узбекистан. Государства, перечисленные в обеих гипотезах, уже подозревались в использовании Pegasus. Третья гипотеза гласит, что ответственность за шпионаж может нести сама Россия.

Галина Тимченко считается ключевым источником информации даже в высших политических кругах Германии и ЕС. Информация и контакты, к которым она и ее СМИ Meduza имеют доступ, потенциально очень важны для многих органов. Берлин – популярное место среди находящихся в изгнании российских журналистов. Многие из них часто встречаются там в различных сверхсекретных местах для обмена информацией и участия в негласных совещаниях.

В 2021 году расследования Forbidden Stories, Süddeutsche Zeitung и других международных СМИ по поводу проекта Pegasus продемонстрировали тревожные масштабы государственной слежки, осуществляемой с помощью шпионской программы Pegasus, автором которой является израильская компания NSO Group. Эта вредоносная программа предоставляет злоумышленникам практически неограниченный и скрытый доступ ко всем данным на зараженных устройствах – электронной почте, зашифрованным сообщениям, чатам, учетным записям и другим сервисам, используемым на устройстве. Помимо этого, Pegasus может активировать камеру и голосовые функции смартфона и вести запись без ведома пользователя. Программа может использоваться даже для управления файлами. [Более 180 журналистов](#) из 20 стран были перечислены как возможные объекты слежки. Организация

RSF подала во Франции иск против компании NSO Group, что стало поводом для [судебного следствия](#).

Одна из основных проблем, связанных с используемыми властями программами-шпионами типа Pegasus, равно как и другими, заключается в том, что эти инструменты являются чрезвычайно сложными и мощными, но в то же время, как их использование практически никак не регулируются. В ответ на эту проблему летом 2022 года RSF открыла [Лабораторию цифровой безопасности](#). Журналисты, опасаясь, что их профессиональное общение может оказаться под цифровым наблюдением, могут обратиться к экспертам берлинского офиса RSF. Кроме того, RSF ведет кампанию за введение во всем мире законодательного контроля за экспортом и продажей подобного шпионского ПО.

После начала агрессии России против Украины, многие российские СМИ и известные журналисты, спасаясь от политических преследований, покинули страну и уехали в Европу. Сейчас, проживая в таких странах как Германия, Латвия и Эстония, они продолжают свою важную работу по обеспечению доступа к независимой информации для русскоязычной аудитории.