FinFisher faces criminal investigation for selling spyware to Turkey without license

The Society for Civil Rights (GFF), Reporters Without Borders Germany (RSF Germany), the European Center for Constitutional and Human Rights (ECCHR) and the blog netzpolitik.org have filed a criminal lawsuit against the German company FinFisher for exporting the spyware FinSpy to Turkey without export license. The public prosecution in Munich, where the FinFisher Company is based, has opened an investigation into the case.

A FinSpy sample found on a Turkish website built the basis for this lawsuit. The Turkish government planted the spyware on a fake version of the Turkish oppositional website *Adalet*. While the original *Adalet* website was intended to help activists coordinate during the protest marches in summer 2017 against president Erdogan, the fake version of the *Adalet* website, offered users a networking application that, once installed, infected their devices with the FinSpy malware.

”It is outrageous and unacceptable to see German spyware being used against journalists and oppositional voices in Turkey“, says Christian Mihr, Executive Director of Reporters without Borders Germany. “This, once again, illustrates the deficiencies of the European export regime of surveillance technology and the dire need for its reform”, he continues.

When used and installed on a recipient’s mobile device, FinSpy enables government authorities access to telephone and VoIP conversations, data systems, screenshots and other photos, GPS data, microphones and connection data as well as to various applications. Consequently, it constitutes a great threat to activists and journalists as it fully exposes their communication with contacts and sources.

Several independent analysts conducted a forensic examination of the malware sample found in Turkey and came to the conclusion that it is a new version of FinSpy. Moreover, time stamps in the code clearly show that this FinSpy malware could not have been coded nor exported before October 2016.

Yet, since 2015, the European Dual-Use regulation as well as the German Foreign Trade and Payments Act require companies to obtain a licence when exporting surveillance technology outside of the EU. The German government has confirmed that it has not granted a single export license for intrusion software since 2015. In Germany, even maintenance and updates of software are subject to licensing. In exporting FinSpy to Turkey FinFisher was acting in clear violation of both German Law and EU regulations, thereby committing a criminal offense.

The FinFisher company has notoriously exported spyware to autocratic regimes. Some of the first rumours of its involvement in supplying tools to authoritarian governments originated from its sales to Middle Eastern governments during the “Arab Spring”. Over the years, the company has solidified its connection to repressive governments, thereby supporting them in brutally cracking down on activists, journalists or anyone critical of the authorities.

That is why GFF, RSF Germany, ECCHR and netzpolitik.org decided to use the analysis of the FinSpy malware found in Turkey to press legal charges against the company and hold it accountable for its involvement in human rights abuses abroad. For violating its obligation to obtain licences for the export of dual-use software in accordance with the German Foreign Trade and Payments Act, the responsible individuals at FinFisher could face a monetary fine or up to 5 years in prison.

This example shows the need for strict and transparent EU-wide regulation on the export of surveillance technology and its enforcement. This fall, the European Council, Commission and Parliament will commence political trialogue negotiations to come to an agreement on the reform of the European Dual-Use regulation.

To download an English version of the full text of the lawsuit click here

For more information, please contact Jennifer Schiementz at presse@reporter-ohne-grenzen.de or under +49 30 609 895 33 55