GlobalResearch
Center for Research on Globalization

How Governments Use Spyware To Attack Free Speech

By Morgan Marquis-Boire
Global Research, August 20, 2015
Amnesty International 20 August 2015

Region: Europe, USA
Theme: Intelligence

Security expert and hacker Morgan Marquis-Boire spends his days researching the shady underworld of government surveillance. Here he explains how governments are using malicious computer code to spy on journalists and human rights activists across the world.

What is spyware and how is it different to malware?

Broadly, malware is malicious code that does something harmful or undesirable on a user's system that runs without their consent. Most people will be familiar with the concept of viruses, trojans, crimeware and even ransomware, which encrypts your data and tries to 'ransom' it back to you. Over the last few years there has been a rise in awareness of malware used for surveillance, or spyware. This is software installed on a victim's computer by state actors, spies and police, rather than cyber criminals. It gives them access to the victim's online communications and, as so much of our lives is now online, this is where most state surveillance now occurs.

How much can they see?

It depends on what you do on the device that has been compromised. For example, as mobile phones have become less about making phone calls and more about general online communication, we've seen a corresponding market for so-called 'lawful intercept' mobile spyware. If you have this type of software surreptitiously installed on your phone it allows people to track your location via GPS, access your contacts list, spy on your SMS messaging, record your phone calls, see what you're talking about on Facebook chat and more.

Spyware on your phone allows people to track your location via GPS, access your contacts list, spy on your SMS messaging and record your calls.

Who is being targeted?

A group of Moroccan journalists and activists known as Mamfakinch were targeted with malware that appears to have been deployed by the Moroccan authorities. They were sent a "bait" document" in the form of a communication pretending to be a news "scoop". When analysed, I found the document contained malicious code that secretly installed spyware on their devices, so the government could see what Mamfakinch were going to be writing and who their sources were.

I also discovered that Ahmed Mansoor, a prominent human rights defender in the United Arab Emirates, has been tracked using commercial spyware. He's constantly subjected to physical and electronic surveillance, and has been beaten and physically assaulted. He has

also received numerous death threats because of his peaceful activism.

During the Arab Spring, the government of Bahrain used spyware sold to them by a UK firm to monitor a group called Bahrain Watch, which tracks arms sales. And in the US, a satellite television station ESAT which reports on Ethiopia was targeted by spyware created by another European company.

Who are the companies selling spyware?

There are smaller players that have become notorious for their sales to repressive regimes. A British-German company Gamma International distributed the spyware used to monitor the activists in Bahrain. Then there's Hacking Team, an Italian company involved in the attack on Mamfakinch and who have previously sold spyware to a variety of repressive governments, including Sudan, Ethiopia, Bahrain, Egypt, Kazakhstan and Saudi Arabia. A recent leak showed that they were contemplating selling to Libya as recently as May this year. And then there are the bigger multinational companies, such as Lockheed-Martin, BAE Systems and Raytheon, who also make this type of technology. This map shows many more of the players operating in the shady surveillance industry.

What can activists and journalists do about it?

The use of protective technologies like encryption, anonymization and privacy tools is pretty low among human rights activists. A lot of people have a good idea of the sensitive information – documents, communications, research – they might want to protect. So the next step is to educate yourself and start thinking sanely about security. There are a number of resources online, such as EFF's comprehensive surveillance self-defence kit. For a quick and simple guide, you can also read this blog post by a colleague from Citizen Lab.

I tend to shy away from broadly advocating individual tools as if they're a panacea, because nothing is a universal surveillance cure-all. People also need to realise they're not only making that decision for themselves, but for other people they're communicating with who may be in a more dangerous situation.

What should Amnesty be doing about it?

I think it's really positive that organisations like Amnesty are starting to speak out about the dangers of surveillance for human rights groups. Amnesty, who have themselves been spied on, know directly what a harmful trend this is. I'm hoping that this will promote a more positive 'security hygiene' in this space. And it's also great that Amnesty is lobbying for more positive policy change in this area too. I'd love to see more transparency around the use of this type of surveillance by governments, as well as a raised awareness among individuals and small organisations about the security measures they should be taking.

What will happen in the future?

It's difficult to look too far in to the future since this is a rapidly changing area of technology. We've seen the NSA say they're going to stop collecting metadata from mobile phones, but on the other side the UK government and the FBI have been fear-mongering about strong encryption on chat and messaging applications and arguing for greater access to users' private data. It's really difficult to predict how this will all pan out, but it's never been more important for people to get involved in the debate and scrutinise what governments are

doing.

Morgan Marquis-Boire is an acting Advisor on Amnesty's Technology and Human Rights Council.
