The Hacking Team and their industry thrive on a climate of fear that they help create

July 13 2015, by David Glance

Surveillance. Credit: Flickr/Fabian

In what has been labelled as poetic justice by some, the Hacking Team, an Italian company that sells mass computer and mobile device surveillance software has itself been hacked. The alleged hackers,

tweeting as Phineas Fisher, uploaded 500GB of internal files stolen from the Hacking Team's systems and made them publicly available.

Details of the Hacking Team's operations and its customers quickly started to emerge. The Hacking Team has sold software to infect, and spy, on around 6,500 devices, by 64 different government security and law enforcement agencies. These governments include those of countries like Chile, Morocco, Tunisia, Sudan, Ethiopia and even Australia and the US.

Statements from Hacking Team representatives have highlighted an ambivalent attitude to who they should or shouldn't sell software to. Company spokesperson Eric Rabe has claimed both that they do vet their clients and follow international trade restrictions and at the same time declared that it is not their job to make judgements about a country's record of human rights abuses.

Even claims that Hacking Team is no longer "servicing" countries like Sudan, whose government has a long history of human rights violations, shows up in a letter from the United Nations, asking whether Sudan was still using its software and the nature of its contracts with that country.

The Hacking Team avoided responding, but eventually argued that, as a private company, it couldn't reveal the nature of its contracts with organisations. And, besides, its software was not a "weapon", and therefore did not contravene any arms embargo placed on the Sudanese government.

Companies selling tools for spying on computers and phones have been around as long as there have been those devices. There are a large number of these companies selling billions of dollars worth of surveillance software to government security agencies and law enforcement relatively indiscriminately.

The software that they sell is capable of getting around encrypted communications and record conversations, use the cameras on phones and computers and remain undetected by antivirus software.

In fact, the rise in use of secure communications like SSL and encryption by default by companies like Google and Apple have been used as a sales technique by stoking fears that this will be used by terrorists to avoid detection by security and law enforcement agencies. They have stoked these fears further by suggesting that, through the hack, its software would now be in the hands of "Terrorists, extortionists, and others" leading to an "extremely dangerous situation".

It is probably not an exaggeration on its part to state that we are in a dangerous situation as a result of the use of this type of software. However, software based "weaponry" is much harder to guard than its physical counterpart, and it is inevitable that through one means or another it will fall into the "wrong hands".

This is made much easier the more widespread the use of this software becomes. The eagerness of agencies to use this method of surveillance inadvertently increases the risk that it will in turn be used against themselves and others.

None of these considerations matter much to the spyware industry. They will thrive in an environment of increased fear and the desire of governments to control opposition and dissent of any kind. The more cyberattacks there are on their customers and companies in their customers' countries, the more their products can be sold as a means of "offensive security".

Despite questions being raised in the European Parliament about the activities of the Hacking Team, it will presumably be back in operation and resuming operations soon. The hack of its documents at least

provides a transparency of its modes of operation that perhaps will reign in its activities with governments with poor human rights records. Given that ultimately, this is all about making money, it is unlikely that it will do this voluntarily.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: The Hacking Team and their industry thrive on a climate of fear that they help create (2015, July 13) retrieved 4 May 2024 from https://phys.org/news/2015-07-hacking-team-industry-climate.html