

## Hacking Team and Boeing Subsidiary Envisioned Drones Deploying Spyware

**18. Juli 2015**

Cora Currier, The Intercept

There are lots of ways that government spies can attack your computer, but a U.S. drone company is scheming to offer them one more. Boeing subsidiary Insitu would like to be able to deliver spyware via drone.

The plan is described in internal emails from the Italian company Hacking Team, which makes off-the-shelf software that can remotely infect a suspect's computer or smartphone, accessing files and recording calls, chats, emails and more. A hacker attacked the Milan-based firm earlier this month and released hundreds of gigabytes of company information online.

Among the emails is a recap of a meeting in June of this year, which gives a "roadmap" of projects that Hacking Team's engineers have underway.

On the list: Develop a way to infect computers via drone. One engineer is assigned the task of developing a "mini" infection device, which could be "ruggedized" and "transportable by drone (!)" the write-up notes enthusiastically in Italian.

The request appears to have originated with a query from the Washington-based Insitu, which makes a range of unmanned systems, including the small ScanEagle surveillance drone, which has long been used by the militaries of the U.S. and other countries. Insitu also markets its drones for law enforcement.

An Insitu engineer wrote to Hacking Team this April: "We see potential in integrating your Wi-Fi hacking capability into an airborne system and would be interested in starting a conversation with one of your engineers to go over, in more depth, the payload capabilities including the detailed size, weight, and power specs of your Galileo System." (Galileo is the name of the most recent version of Hacking Team's spyware, known as Remote Control System.)

In an internal email, a Hacking Team account manager suggests that they could do so using a "TNI," or "tactical network injector." A TNI is a portable, often laptop-based, physical device, which an operator would use to plug into a network the target is using — such as an open Wi-Fi network in a hotel or coffee shop. When the targeted person uses the Internet for some ordinary activity, like watching a video or downloading an app, the device intercepts that traffic (so long as it is unencrypted) and injects the malicious code that secretly installs Hacking Team's spyware. (For more technical details on network injectors, see The Intercept's previous reporting.)

Presumably, attaching a small network injector to a drone would give the ability to attack Wi-Fi networks from above, or at a greater distance. The system operator wouldn't have to get physically near the target. Insitu did not respond to The Intercept's requests for comment.

Hacking Team gained notoriety in recent years as human rights and digital security advocates found traces of its spyware on the computers of journalists and political activists from Ethiopia, Morocco and elsewhere. As The Intercept reported last week, the leaked files confirm that Hacking Team sold to many countries with dubious human rights records, and also to agencies in the U.S., where the use of such spyware is still the subject of legal controversy.