Spy Tech Company 'Hacking Team' Gets Hacked

By Lorenzo Franceschi-Bicchierai

Published: 2015-07-06 · Archived: 2026-04-05 13:16:32 UTC

Sometimes even the cops get robbed.

The controversial Italian surveillance company Hacking Team, which sells spyware to governments all around the world, including agencies in Ethiopia, Morocco, the United Arab Emirates, as well as the US Drug Enforcement Administration, appears to have been seriously hacked.

Videos by VICE

Hackers have made 500 GB of client files, contracts, financial documents, and internal emails, some as recent as 2015, publicly available for download.

Hacking Team's spokesperson Eric Rabe did not immediately respond to Motherboard's calls and email asking for verification that the hacked information is legitimate. Without confirmation from the company itself, it's difficult to know what percentage of the files are real—however, based on the sheer size of the breach and the information in the files, the hack appears to be authentic.

What's more, the unknown hackers announced their feat through Hacking Team's own Twitter account.

The hackers composed the tweets as if they were written by Hacking Team. "Since we have nothing to hide, we're publishing all our e-mails, files, and source code," the hackers wrote in a tweet, which included the link to around 500 Gb of files.

The hackers also started tweeting a few samples of internal emails from the company. One of the screenshots shows an email dated 2014 from Hacking Team's founder and CEO David Vincenzetti to another employee. In the email, titled "Yet another Citizen Lab attack," Vincenzetti links to a report from the online digital rights research center Citizen Lab, at the University of Toronto's Munk School of Global Affairs, which has exposed numerous cases of abuse from Hacking Team's clients.

Hacking Team has never revealed a list of its clients, and has always and repeatedly denied selling to sketchy governments, arguing that it has an internal procedure to address human rights concerns about prospective customers.

The email about Citizen Lab is filed in a folder called "Anti HT activists." Claudio Guarnieri, a security researcher who has investigated Hacking Team along with others at the Citizen Lab, was quick to point this out.

> Interesting, we fall under the
>
> ClaudioJuly 6, 2015

It's unclear exactly how much the hackers got their hands on, but judging from the size of the files, it's certainly a large collection of internal files. A source who asked to speak anonymously due to the sensitivity of the issue, told me that based on the file names and folders in the leak, the hackers who hit Hacking Team "got everything."

A few hours after the initial hack, a list of alleged Hacking Team customers was posted on Pastebin. The list includes past and current customers. Among the most notable, there are a few that were previously unknown, such as the FBI, Chile, Australia, Spain, and Iraq, among others.

We reached out to the hackers via direct message on Twitter, asking if they could comment. Their initial response, "sure, we got such good publicity from your last story!" referred to Motherboard's report from April, which revealed that the DEA had secretly purchased Hacking Team's software for $2.4 million.

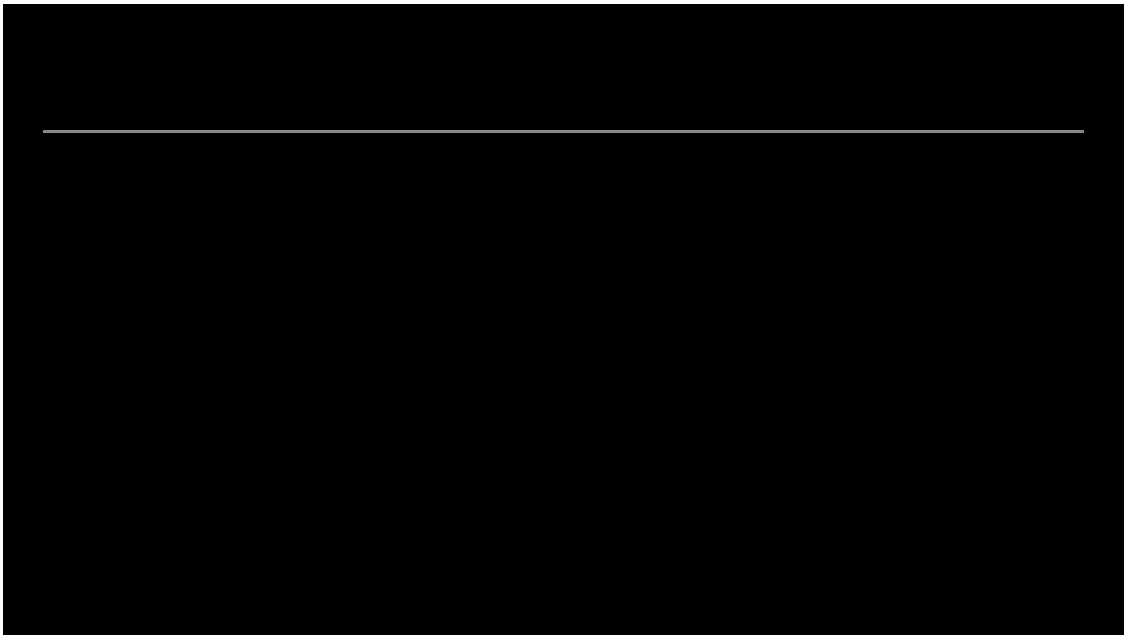
The hacker, or hackers, however, declined to comment for now.

Many security researchers and human rights activists reacted to the hack with sarcasm.

We also reached out to Vincenzetti, asking for his comments and reactions, and will update when and if we hear back. (In the past, Vincenzetti wrote on a mailing list that "[Motherboard] never reports on Hacking Team without smug editorial comment," so we're not holding out our breath.)

The breach on Hacking Team comes almost a year after another surveillance tech company, the competing FinFisher, was hacked in a similar way, with a hacker leaking 40 Gb of internal files.

FinFisher, like Hacking Team, sells surveillance software to law enforcement agencies across the world. Their software, once surreptitiously installed on a target's cell phone or computer, can be used to monitor the target's communications, such as phone calls, text messages, Skype calls, or emails. Operators can also turn on the target's webcam and exfiltrate files from the infected device.



In one alleged internal email leaked today, Hacking Team's Vincenzetti gloated over FinFisher's hack, writing that "a wannabe competitor of ours has been severely hacked."

It seems that Hacking Team has suffered the same fate.

This story has been updated to include information about the list of Hacking Team customers, and to add a comment from a source on the extent of the damage.
