

Internet watchdog Citizen Lab targeted in comically inept undercover sting

reader comments

37 with 28 posters participating

Share this story

It was almost like an episode of *Spy vs. Spy*—a security researcher conceals a camera on his person to record an undercover operative who, under false pretenses and with his own hidden camera, quizzes the researcher about work he did exposing an Israeli exploit seller with highly questionable ethics.

In fact, the counter-sting happened earlier this month, according to an article published Friday by the Associated Press. Researchers at Internet watchdog group Citizen Lab orchestrated the sting after they grew suspicious of a man calling himself Michael Lambert who contacted Citizen Lab researcher John Scott-Railton to request a lunch meeting at a swanky Toronto hotel. The suspicions were fueled by an earlier meeting in December, in which a man masquerading as a socially conscious investor named Gary Bowman grilled a different Citizen Lab researcher about work the watchdog did exposing NSO Group, the Israeli exploit seller.

Scott-Railton agreed to the Toronto meeting and was outfitted with a GoPro action camera and several recording devices. At the lunch, he spotted a tiny camera poking out from a pen

Lambert had placed on the table. As the AP reports:

Lambert didn't seem to be alone. At the beginning of the meal, a man sat behind him, holding up his phone as if to take pictures and then abruptly left the restaurant, having eaten nothing. Later, two or three men materialized at the bar and appeared to be monitoring proceedings.

Scott-Railton wasn't alone either. A few tables away, two Associated Press journalists were making small talk as they waited for a signal from Scott-Railton, who had invited the reporters to observe the lunch from nearby and then interview Lambert near the end of the meal.

The conversation began with a discussion of kites, gossip about African politicians, and a detour through Scott-Railton's family background. But Lambert, just like Bowman, eventually steered the talk to Citizen Lab and NSO.

"Work drama? Tell me, I like drama!" Lambert said at one point, according to Scott-Railton's recording of the conversation. "Is there a big competition between the people inside Citizen Lab?" he asked later.

Like Bowman, Lambert appeared to be working off cue cards and occasionally made awkward conversational gambits. At one point he repeated a racist French expression, insisting it wasn't offensive. He also asked Scott-Railton questions about the Holocaust, anti-Semitism, and whether he grew up with any Jewish friends. At another point he asked whether there might not be a "racist element" to Citizen Lab's interest in Israeli spyware.

After dessert arrived, the AP reporters approached Lambert at his table and asked him why his company didn't seem to exist.

He seemed to stiffen.

"I know what I'm doing," Lambert said, as he put his

files—and his pen—into a bag. Then he stood up, bumped into a chair and walked off, saying “Ciao” and waving his hand, before returning because he had neglected to pay the bill.

NSO first came to mass attention in 2016 when researchers from Citizen Lab and mobile security provider Lookout found highly advanced spyware targeting an iPhone belonging to a political dissident located in the United Arab Emirates. Dubbed Pegasus, it was among the most sophisticated pieces of mobile spyware ever found in the wild. To surreptitiously infect the targeted iPhone with nothing more than a clicking of an SMS message link, Pegasus chained together three distinct exploits.

“Pegasus is the most sophisticated attack we’ve seen on any endpoint because it takes advantage of how integrated mobile devices are in our lives and the combination of features only available on mobile—always connected (Wi-Fi, 3G/4G), voice communications, camera, email, messaging, GPS, passwords, and contact lists,” Lookout and Citizen Lab researchers wrote. “It is modular to allow for customization and uses strong encryption to evade detection.”

Last October, Citizen Lab described how a fake package-delivery notification infected the iPhone belonging to Omar Abdulaziz (a confidant of the late Jamal Khashoggi) with NSO’s Pegasus spyware. Abdulaziz later said the hack played a major role in Khashoggi’s brutal killing because the spyware exposed private messages in which Khashoggi bluntly criticized the Saudi royal family.

Friday’s article doesn’t say who the the undercover operatives worked for. Representatives of NSO categorically denied having any role, direct or otherwise, in the undercover incidents. Citizen Lab has posted supporting transcripts and emails related to the undercover sting [here](https://arstechnica.com/?p=1446883).

<https://arstechnica.com/?p=1446883>