Italian surveillance firm's breach puts spies in hot seat (Update)

July 16 2015, byRaphael Satter

A dramatic breach at an Italian surveillance company has laid bare the details of government cyberattacks worldwide, putting intelligence chiefs in the hot seat from Cyprus to South Korea. The massive leak has already led to one spymaster's resignation—and pulled back the curtain on espionage in the iPhone age.

More than 1 million emails released online in the wake of the July 5 breach show that Hacking Team sold its spy software to the FBI and to Russian intelligence. It worked with authoritarian governments in the Middle East and pitched to police departments in the American suburbs. It even tried to sell to the Vatican—all while devising a malicious Bible app to infect religiously minded targets.

"It's a mini-Snowden event," said Israel-based security researcher Tal Be'ery, likening the impact of the leak to the publication of top secret NSA documents by former intelligence worker Edward Snowden.

Like others, Be'ery long suspected the world's security agencies of hacking, but he said he was struck by "the ubiquity of it—used on all continents, by both democracies and dictatorships."

Invoices from Sudan's intelligence service and a Russian arms conglomerate have critics—including a European parliamentarian—asking whether the company flouted international sanctions. A client list that includes Uzbekistan, Egypt and Azerbaijan has reinforced worries from groups such as Privacy International that the

spyware is being used to silence dissidents. And 'we-love-your-stuff' emails from sheriffs, police and prosecutors across the United States suggest local law enforcement is eager to give the program a test drive.

Hacking Team's spyware was used by a total of 97 intelligence or investigative agencies in 35 countries, according to South Korean National Intelligence Service chief Lee Byoung Ho, who explained himself to lawmakers Tuesday after it became clear his organization was among the Milan-based company's clients.

Hacking Team did not immediately return emails seeking comment Thursday, but the company denies allegations of sanctions-busting and other wrongdoing.

Speaking to Italian newspaper La Stampa over the weekend, Chief Executive David Vincenzetti said the spyware is used to fight terror and "root out lone wolves."

"We're the good guys," he said.

Hacking Team's spyware is called Remote Control System and is delivered to targets through a mix of malicious links, poisoned documents and pornography, the emails show. Booby-trapped programs could be tailored to targets of any persuasion; some messages appear to show Hacking Team working on apps named "Quran" and "DailyBible."

Once secretly installed, the spyware acts as a track-anything surveillance tool.

The emails show Kazakhstan's spy agency trying to suck chat histories from a target's Samsung smartphone and Saudi Arabia's Interior Ministry using an infected handset as a tracking beacon. They also show Mongolia's anti-corruption authority trying to steal a target's Facebook

password by logging his keystrokes and Czech police at work turning a BlackBerry's microphone into an ad-hoc listening device. Vincenzetti told La Stampa the spyware even had the ability to automatically take pictures of people's faces as they picked up their phones.

Mexico is a particularly aggressive user of the technology, according to a leaked client list. In Ecuador, evidence that Hacking Team's spyware was used by the country's SENAIN spy agency has caused an uproar.

Senior police and intelligence figures have been quizzed about Hacking Team by lawmakers in Italy and the Czech Republic. Revelations that the Cyprus Intelligence Service has been secretly using the spyware prompted the resignation of the agency's boss, Andreas Pentaras, over the weekend.

The targets of all this spying are rarely made explicit. But in one of the leaked emails, dated Dec. 15, 2014, Vincenzetti suggests he sometimes has a pretty good idea of who is being hacked.

"I usually get a call from, say, the Head of Italian Police's Deputy and he tells me: 'Congratulations, Mr. Vincenzetti!'. I tell him: 'Thank you Sir, may I ask you what are you referring to?' 'I am talking to what you will read tomorrow morning on the front pages of all the newspapers!' he laughs. And he hangs up. And the day after I read that a mafia boss has been finally arrested, that an apparently impossible investigation mystery on a savage assassination has been finally solved and the murderer arrested, etc."

Vincenzetti suggested the rest of the world was being kept in the dark about government cyberattacks.

Authorities "never disclose how they did it because they want to protect our technology and they want to protect us," he said.

For researchers like Be'ery, the leak has provided unprecedented insight into how governments hack. For human rights workers, it has confirmed their fears about state surveillance. And for past victims of Hacking Team's software—people like prominent Emirati blogger Ahmed Mansoor—the leak has provided a dose of schadenfreude.

"They can at least understand how it feels to encroach into somebody's privacy," he said.