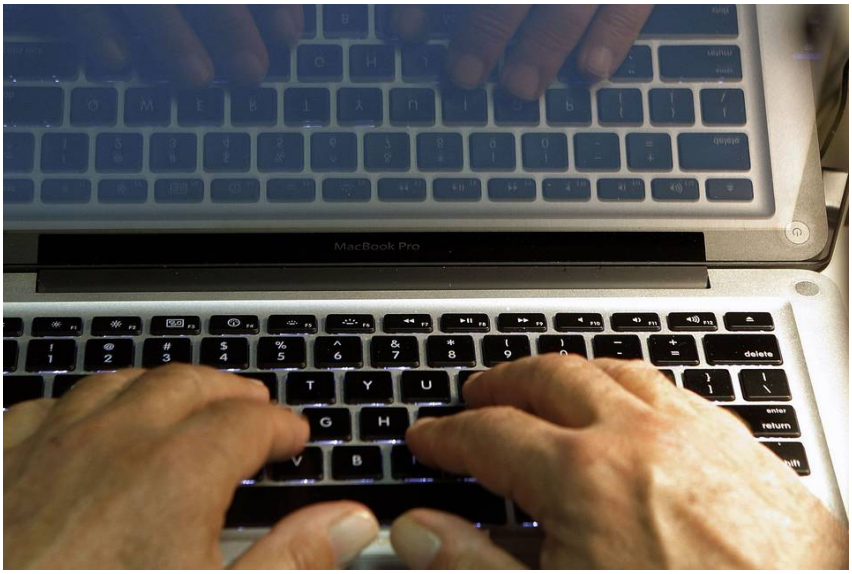
THE WALL STREET JOURNAL.

http://www.wsj.com/articles/hacking-software-maker-gets-hacked-1436223757

TECH

Hacking Team, the Surveillance Tech Firm, Gets Hacked

Italian company sold surveillance tools to dozens of countries, according to leaked files



The industry that sells software allowing governments to hack into computers has come under fire over allegations that the technology is used by repressive regimes to target dissidents, journalists and others. *PHOTO: DAMIAN DOVARGANES/ASSOCIATED PRESS*

By **JENNIFER VALENTINO-DEVRIES** and **DANNY YADRON**
July 6, 2015 8:48 p.m. ET

A company that sells software allowing governments to hack into computers has itself been hacked, and files posted late Sunday indicate it sold surveillance technology to dozens of countries, including Sudan, Egypt, Russia and the U.S.

The Italian company, Hacking Team, or HT S.r.l., is among a handful of companies that offer such surveillance tools to law enforcement around the world. The company's techniques are similar to those used in "malware" by criminals trying to steal computer users' personal information.

The market for off-the-shelf surveillance tech, including such software, has grown. In 2011, an industry veteran estimated it at $5 billion a year, The Wall Street Journal reported.

Hacking Team says its tools enable investigators to obtain information even if targets encrypt their communications to protect them.

RELATED

- When Does a Hack Become an Act of War? (http://www.wsj.com/articles/when-does-a-hack-become-an-act-of-war-1434189601) (June 13)
- Three Months Later, State Department Hasn't Rooted Out Hackers (http://www.wsj.com/articles/three-months-later-state-department-hasnt-rooted-out-hackers-1424391453) (Feb. 19)
- Hacking Trail Leads to Russia, Experts Say (http://www.wsj.com/articles/hacking-trail-leads-to-russia-experts-say-1414468869) (Oct. 28, 2014)
- Document Trove Exposes Surveillance Methods (http://www.wsj.com/articles/SB10001424052970203611404577044192607407780) (Nov. 29. 2011)

The industry has come under fire over allegations that the software is used by repressive regimes to target dissidents, journalists and others. Hacking Team says on its website it doesn't sell to countries if there are "credible concerns" that its products "will be used to facilitate human rights violations."

In a 2011 interview with The Wall Street Journal, Marco Valleri, a Hacking Team co-founder, said the company was "fully compliant" with international laws. "Europe and the U.S. both have blacklists of countries that are not so friendly. We are allowed to sell only to friendly countries," he said.

A 2014 report by the Citizen Lab at the University of Toronto found indications that Hacking Team's products were used in Ethiopia, Sudan, Oman, Egypt and elsewhere. Those researchers said the company's software was used in attempts to hack Ethiopian journalists in the U.S. Hacking Team at the time said it didn't sell services to repressive regimes.

The documents posted Sunday include invoices and ledgers that appear to record sales to Sudan, Azerbaijan and Egypt, among others.

Officials from these countries couldn't immediately be reached for comment.

Hacking Team's U.S. spokesman, Eric Rabe, said the company "is investigating" and that it doesn't "confirm the identities of clients or their locations." He didn't respond

directly to a question about the authenticity of the documents.

"We consider this to be an illegal attack and theft and certainly a violation of law," Mr. Rabe said. He also said that "with our systems under attack" the company has recommended that clients suspend investigations temporarily until the company can fully understand the exposure.

The documents posted online on a New Zealand file-hosting service include what appears to be a 2012 invoice from Hacking Team to InfoTeCS JSC, a Russian computer-security company that on its website boasts of licenses from Russia's Federal Security Service and Ministry of Defense to produce encryption and protect state secrets.

InfoTeCS appeared to pay the bill. In November 2013, Hacking Team sent a document for a one-year renewal. InfoTeCS didn't respond to a request for comment.

Other documents relate to possible sales to Sudan, which has been accused of torture and targeting political foes and has been under a United Nations arms embargo for the past decade. They include two 2012 invoices to Sudan's National Intelligence and Security Services, and communications from the U.N. panel overseeing sanctions.

In the letters, U.N. representatives say such software may be considered military equipment and thus prohibited. Hacking Team argues that its software isn't a weapon or military equipment and thus not regulated by the embargo.

In the letters, the company says it doesn't have a relationship with Sudan, but declines to discuss past conduct.

Mr. Rabe said that, in the past, Hacking Team "took the position that our software is not equivalent to fighter planes, rockets, or bombs." Since January, he said, the company has been regulated by new international protocols for technology that can have both civil and military uses.

"We have worked with the Italian government and fully implemented this protocol," he said.

U.N. representatives didn't immediately comment on the documents.

Computer-security researchers said the disclosures could intensify the debate around the sale of such surveillance tools.

"I don't think there's anyone who sells surveillance software who isn't aware of the

human-rights implications," said Morgan Marquis-Boire, a senior researcher at Citizen Lab who investigated the Hacking Team tools.

He said proposals to limit the exchange of hacking tools are controversial because they could also prevent computer researchers from sharing information across borders.

The disclosed documents also appear to show sales to U.S. agencies. Hacking Team has an office in Annapolis, Md., to target North and South America. A "client overview list" shows sales of software licenses and maintenance from 2011 through 2015 to the U.S. Federal Bureau of Investigation and Drug Enforcement Administration totaling more than $1 million. In 2013, the DEA received a $170,000 bill for software renewal, an upgrade and "training in Bogota," according to one file.

The U.S. Justice Department didn't immediately respond to a request for comment.

Write to Jennifer Valentino-DeVries at Jennifer.Valentino-DeVries@wsj.com and Danny Yadron at danny.yadron@wsj.com