technology review
Published by MIT

Close Window

Advertisement

Tuesday, December 6, 2011

The Cyber Security Industrial Complex

Documents point to a huge industry that provides online surveillance tools to governments and police agencies.

By David Talbot

A claim by Wikileaks that documents it released last week provide evidence of a "secret new industry" of mass surveillance was as breathless as previous pronouncements from Julian Assange's organization. But the material does provide a stark reminder that our online activities are easily snooped upon, and suggests that governments or police around the world can easily go shopping for tools to capture whatever information they want from us.

The take-home for ordinary computer users is that the privacy and security safeguards they use—including passwords and even encryption tools—present only minor obstacles to what one researcher calls the "cyber security industrial complex."

"There is no true privacy in any computing systems against determined government-level surveillance," says Radu Sion, a computer scientist at Stony Brook University who directs its Network Security and Applied Cryptography Laboratory. He says that as computing systems become more complex, and reliant on components from many different suppliers, the number of vulnerabilities that can be exploited by attackers and surveillance tools will grow.

The 287 documents released by Wikileaks come from 160 companies in 25 countries. They detail various commercial products and services offered to governments and law enforcement officials interested in intercepting online communications or eavesdropping on computer use. Wikileaks founder Julian Assange described the documents as unmasking a "international mass surveillance industry." In fact, many of the companies named have been discussed in public before, for example, Blue Coat, a U.S. company whose corporate network filters have been used by the Syrian regime to censor the Internet inside the nation's borders and spy on dissidents. However, the Wikileaks release was still noteworthy because of its breadth and level of detail.

Marketing materials from a German company, DigiTask, are a typical offering from the new Wikileaks haul. They describe how the company's software—installed on users' computers by taking advantage of newly found software defects known as "zero day exploits"—could steal encryption keys to let law enforcement or governments eavesdrop. The same method was used against security software company RSA earlier this year in an apparent attempt to compromise U.S. defense contractors.

The Wikileaks release also included material from Paladion, based in India, containing claims that the company could trace encrypted banking transactions and Gmail messages.

Ron Deibert, director of Internet think-tank Citizen Lab at the University of Toronto, has long studied the global spread of such technologies and their ready adoption by governments. The technologies on offer include social networking mapping, cell phone tracking, location tracking, and so-called "deep packet inspection" techniques used to read the content of passing Internet traffic.

The growing role of the Internet in everyday life and business is creating a rich trove of digital information about people, companies, and nations, Deibert noted in a recent blog post. "Unsurprisingly, a massive cyber industrial complex has sprouted around the commercial exploitation of [it]," he wrote. Deibert notes that censoring the Web used to be considered an undertaking for only hubristic, authoritarian regimes, but is now being considered by defense departments worldwide being courted by corporations like those featured in the new Wikileaks documents.

Copyright Technology Review 2011.