Researchers find German-made spyware across globe (Update 2)

March 13 2013, by Raphael Satter

The discovery of a group of servers linked to an elusive espionage campaign is providing new details about a high-tech piece of spy software that some fear may be targeting dissidents living under oppressive regimes.

A Canadian research center said Wednesday that it had identified 25 different countries that host servers linked to FinFisher, a Trojan horse program which can dodge anti-virus protections to steal data, log keystrokes, eavesdrop on Skype calls, and turn microphones and webcams into live surveillance devices.

Citizen Lab, based at the University of Toronto's Munk School of Global Affairs, said that Canada, Mexico, Bangladesh, Malaysia, Serbia, and Vietnam were among the host countries newly identified in Wednesday's report. That alone doesn't necessarily mean those countries' governments are using FinFisher, a program distributed by British company Gamma International, but it is an indication of the spyware's reach.

Morgan Marquis-Boire, the report's lead author, said his goal was "to show the proliferation of this type of active intrusion and surveillance." In telephone interview, he said that the world of government surveillance was changing and urged journalists, aid workers, and activists to take note.

"It's not just phone tapping," he said. "It's installing a backdoor on your computer to record your Skype conversations and go through your

email."

Advocacy group Privacy International described the report as evidence that Gamma had sold FinFisher to repressive regimes, calling it a "potential breach of UK export laws."

Gamma did not comment on the report.

The company, based in the English town of Andover, has come under increasing scrutiny after a sales pitch for the spyware was recovered from an Egyptian state security building shortly after the toppling of dictator Hosni Mubarak in 2011. Reporting by Bloomberg News subsequently identified opposition activists from the Persian Gulf kingdom of Bahrain as targets of the company's surveillance software.

The discovery of FinFisher servers in countries run by authoritarian governments—such as Turkmenistan and Ethiopia—have raised further questions about the company's practices. On Tuesday, Paris-based journalists' rights group Reporters Without Borders named Gamma one of its five "corporate enemies of the Internet."

The report said evidence for the Ethiopian government's use of FinFisher was particularly strong, explaining that Citizen Lab had found an example of the spyware which spread through a booby-trapped email purporting to carry images of Ethiopian opposition figures. Once the Trojan was downloaded, it would connect to a server being hosted by Ethiopia's national telecommunications provider, Ethio Telecom.

It's not clear who the Trojan's intended targets might have been, although online messages have provided key evidence in several recent terror cases that have resulted in the incarceration of media and opposition figures.

Journalist Reyot Alemu was arrested in 2011 after she was caught attempting to anonymously email articles to a U.S.-based opposition website, while opposition leader Andualem Arage is currently appealing the life sentence he received last year after authorities got hold of his Skype conversation with an alleged enemy of the Ethiopian state.

Ethiopian opposition leader and Bucknell University academic Berhanu Nega said he had no proof that he or his colleagues had been hacked by the Ethiopian government, but he said he wouldn't be surprised.

He said opposition figures had long been careful on the phone or over email, but he called FinFisher "the most pervasive kind of spying that we have been confronted with.

"We're now trying to clear our computers."

There was little comment on FinFisher from Ethiopian officials. A spokesperson for Ethio Telecom could not be reached, and Deputy Prime Minister Debretsion Gebremichael said in an email that his department "is not aware of such (a) product" and referred questions about it to Gamma. Gamma referred questions to FinFisher's German developer, Martin Muench.

Muench did not return several emails seeking comment but, in a recent interview with German newspaper Suddeutsche Zeitung, he defended his work as part of the fight against crime.

"I think it's good when the police do their job," Muench told the daily. He dismissed the notion that what he was doing was violating anyone's human rights.

"Software doesn't torture anybody," he said.

More information: Citizen Lab report: citizenlab.org/2013/03/you-onl … bal-proliferation-2/
Gamma's description of FinFisher: www.finfisher.com/FinFisher/en/index.php
Reporters Without Borders on why Gamma is an "enemy of the Internet": surveillance.rsf.org/en/gamma-international/