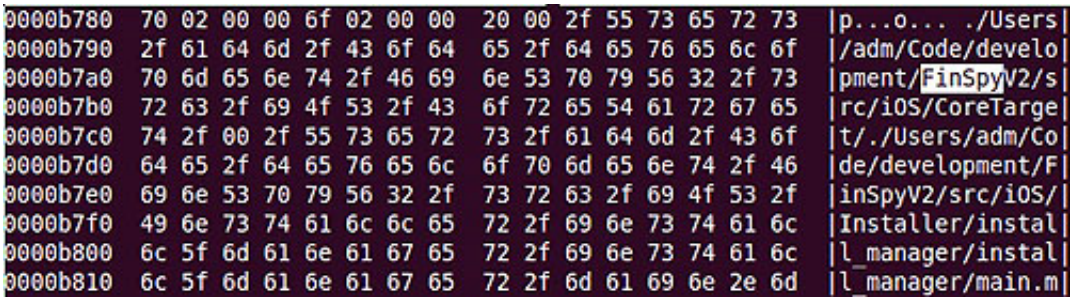
Toronto study shows mobile spyware's long shadow

September 1 2012, by Nancy Owano



(Phys.org)—Spyware sold legally can infect BlackBerrys, iPhones, and other mobile devices, according to a study from two security researchers at the University of Toronto Munk School of Global Affairs' Citizen Lab. Morgan Marquis-Boire and Bill Marczak, in their study "The SmartPhone Who Loved Me: FinFisher Goes Mobile?" focus on spyware that can be used by governments as well as law enforcement to commandeer phones. They analyzed samples that appear to be variants of the FinFisher toolkit. They identified various command and controls servers as well. They sought to follow the marks of spyware surveillance software from Bahrain across several continents.

Earlier this year, researchers had noted how activists in Bahrain were spied on with the software. They suggested that it appeared to be FinSpy, part of the FinFisher commercial surveillance toolkit. The Citizen Lab

workers said they now also recovered versions of the spyware that target the BlackBerry OS, Windows Mobile, Nokia's Symbian platform, as well as Android, and that it has seen "structurally similar" Android spyware communicating with command-and-control servers in the United Kingdom and the Czech Republic.

As for Apple devices, it appears that FinFisher spyware will run on iPhone 4, 4S, iPad 1, 2, 3, and iPod touch 3, 4 on iOS 4.0 and up.

FinFisher spyware comes from Gamma International in Andover, UK, part of the Gamma Group of companies. The company defines its FinFisher portfolio as "intrusion products" offered to "law enforcement and intelligence agencies." Outsiders are worried that such a tool sold in the marketplace for off the shelf computer surveillance can be not only used by law enforcement agencies going after human trafficking, child molesters and criminals but also by repressive governments keeping a lid on all manner of dissent. The two researchers now find that mobile versions of spyware have been customized, regardless of phone brand, for all the major mobile phones.

Earlier this year, the researchers had pointed out that Bahrain dissenters had started getting e-mails with suspicious attachments: An intended target gets an email or text message on the phone, and clicks the included link. The page that loads drops malicious code that pops up a fake system to update a message. If the user clicks on it, the spyware app is installed. What happens after that: the remote system can record from the microphone, track locations, and monitor communications. In a previous report, "From Bahrain with Love: FinFisher's Spy Kit Exposed?" the researchers characterized the malware, and they suggested that it appeared to be FinSpy, part of the FinFisher product line. (Note the question marks used in titles for the two studies.)

Gamma's response, however, was that FinFisher was never sold to

Bahrain. According to the company, a copy might have been stolen and re-engineered for some unauthorized use.

Morgan Marquis-Boire is a Technical Advisor at the Citizen Lab, Munk School of Global Affairs, University of Toronto. He works as a security engineer at Google. Bill Marczak is a computer science Ph.D student at UC Berkeley and founding member of Bahrain Watch.

More information: citizenlab.org/2012/08/the-sma … nfisher-goes-mobile/
www.bloomberg.com/news/2012-07 … -be-stolen-copy.html