GlobalResearch
Center for Research on Globalization

Hacking Team Malware Targeted Saudi Arabia Protestors

By Pratap Chatterjee
Global Research, July 03, 2014
CorpWatch 27 June 2014

Region: Middle East & North Africa
Theme: Intelligence, Police State & Civil Rights

Malicious software from Hacking Team of Italy that can be used to spy on cell phones has been found by Citizen Lab activists to have been used to target people in Saudi Arabia. The software was bundled into a fake phone application for Qatif Today, a local news site.

The discovery may shed light on a Wikileaks report that claimed Hacking Team sales people – notably a Lebanese citizen named Mostapha Maanna – made three trips to Saudi Arabia in 2012, soon aftermajor protests in the country.

Hacking Team, a company from Milan, is well known for selling technology to governments that can be used to create emails to target individuals by inviting them to click on a link or attachment which then installs a spy tool called Remote Control System (RCS) on the target's computer. RCS (also known as DaVinci) can then copy the Web browsing history of its targets, turn on their computer microphone and webcam to eavesdrop on them, as well record their conversations on computer applications like Skype.

The new Hacking Team exploit that Citizen Lab researchers discovered was bundled into a fake Android phone app that purported to be from Qatif Today, a news web site in the eastern Saudi province that has a large Shia population.

The fake app was placed in a Dropbox account (since deleted) which visitors to a Twitter account were invited to download in March 2014. Once installed, the software was able to place itself in the heart of the phone where it could secretly make copies of phone activity to forward to two servers – one on Leaseweb in Germany and another on Linode in Japan.

"We found that the apps attempt to access the local files stored by popular social media, chat, and call apps including Facebook, Viber, WhatsApp, Skype, LINE and QQ," wrote the Citizen Lab researchers.

> "In addition, the app accesses the locally stored mail files belonging to the compromised user's mail account. We find a range of audio recording, camera, video, key logging, "live mic," chat, device info etc. configuration settings relevant to the surveillance functionality of the implant. We also see what appear to be, location, screenshot-taking, and browsing activity modules."

"With the internet we thought it was all going to be freedom and freedom of communication," Morgan Marquis-Boire, a researcher at Citizen Lab, told Vice magazine. "But it's giving governments the power to impose ancient ideologies with modern

technology."

Eric Rabe, a Hacking Team spokesman, did not deny the Citizen Lab allegations when asked for comment by the Associated Press. "We believe the software we provide is essential for law enforcement and for the safety of all in an age when terrorists, drug dealers and sex traffickers and other criminals routinely use the Internet and mobile communications to carry out their crimes," Rabe said.

But Citizen Lab noted that the tool appeared to be aimed specifically at Shia dissidents in Saudi Arabia. Notably Qatif has a large Shia population which has long chafed under the Saudi monarchy and started to organize following the Arab Spring protests in 2011, using social media as a key way to distribute information.

Many of the Shia in Saudi Arabia have followed protests in neighboring Bahrain with great interest – not surprisingly where the link to the spy software was placed on a Twitter account with the handle @bh_pearl used by a human rights activist. (The name is a reference to the Pearl Roundabout in central Manama, Bahrain, where many anti-government protests take place)

Articles by: Pratap Chatterjee