Hacking Team Malware Targeting Shia Community in Saudi Arabia

Toronto, Canada (June 24, 2014) – The Citizen Lab is pleased to announce the publication of a report entitled "Police Story: Hacking Team's Government Surveillance Malware" — the latest in our series of reports into Hacking Team's Remote Control System (RCS) interception tool. This work builds on our previous research into the technologies and companies behind "lawful interception" malware. This technology is marketed as filling a gap between passive interception (such as network monitoring) and physical searches. In essence, it is malware sold to governments.

The report is divided into two parts. In Part 1, we analyze our discovery of an Android application called Qatif Today that is bundled with a Hacking Team payload. The app provides news and information in Arabic with a special relevance to the Qatif Governorate of Saudi Arabia, which is a predominantly-Shia community. A number of reasons for political tensions exist, ranging from demographic pressures, cost of housing, and unemployment, to issues of women's and minority rights. The Shia community in the province has long-standing grievances over perceived political and cultural marginalization by the Sunni ruling regime. Although we are not in a position to determine the identity of the group or individual targeted with this malware, we speculate that the attack may be linked to political protest in eastern Saudi Arabia. In Part 2, we provide a general overview of some of the functionality and specifics of the RCS, according to documents we found in the wild.

This report is part of our series of reports on Hacking Team and companies of their ilk. We expose their global proliferation and highlight the technologies and tactics that they use, not only because they create the most sophisticated implants, but also because they appear to be used exclusively by the countries they are attributed to, and are designed to perform targeted intrusions. By dramatically lowering the entry cost on invasive and hard-to-trace monitoring, the equipment lowers the cost of targeting political threats.

About the Citizen Lab

The Citizen Lab at the Munk School of Global Affairs, University of Toronto is an interdisciplinary laboratory that explores the intersection of information technology, global security, and human rights. In 2009, the Citizen Lab was part of a research team that produced the *Tracking Ghostnet* cyber espionage report, one of the first public reports to document a major cyber espionage network affecting thousands of computers in dozens of high-profile targets worldwide. The Citizen Lab has also published a series of reports that document the emerging market for lawful intercept technologies, what some call "digital arms," targeting civil society organizations. In 2014, the Citizen Lab was the first Canadian organization to be awarded the prestigious John D. and Catherine T. MacArthur Award for Creative and Effective Institutions.

-30-

For more information, contact:
Irene Poetranto
Communications Officer
Citizen Lab and Canada Centre for Global Security Studies
Munk School of Global Affairs
University of Toronto

Tel: 416-946-8903
irene.poetranto@utoronto.ca