Mapping Hacking Team's Covert Surveillance Networks

Toronto, Canada (February 19, 2014) - Hacking Team, also known as HT S.r.l., is a Milan-based purveyor of "offensive technology" to governments around the world. One of their products, Remote Control System (RCS), is a trojan that is sold exclusively to intelligence and law enforcement agencies worldwide.

This report, entitled "Mapping Hacking Team's "Untraceable" Spyware," is the second in a series of reports that focus on the global proliferation and use of RCS spyware. Read the first report, "Hacking Team and the Targeting of Ethiopian Journalists" and its coverage in the Washington Post.

This report maps out covert networks of "proxy servers" used to launder data that RCS exfiltrates from infected computers, through third countries, to an "endpoint," which we believe represents the spyware's government operator; this process is designed to obscure the identity of the government conducting the spying. For example, data destined for an endpoint in Mexico appears to be routed through four different proxies, each in a different country. This so-called "collection infrastructure" appears to be provided by one or more commercial vendors — perhaps including Hacking Team itself.

Hacking Team advertises that their RCS spyware is "untraceable" to a specific government operator. However, we claim to identify a number of current or former government users of the spyware by pinpointing endpoints, and studying instances of RCS that we have observed.

We suspect that agencies of these 21 governments are current or former users of RCS: Azerbaijan, Colombia, Egypt, Ethiopia, Hungary, Italy, Kazakhstan, Korea, Malaysia, Mexico, Morocco, Nigeria, Oman, Panama, Poland, Saudi Arabia, Sudan, Thailand, Turkey, UAE, and Uzbekistan. Nine of these countries receive the lowest ranking, "authoritarian," in The Economist's 2012 Democracy Index. Additionally, two current users (Egypt and Turkey) have brutally repressed recent protest movements.

We also study how governments infect a target with the RCS spyware. We find that this is often through the use of "exploits" — code that takes advantage of bugs in popular software. Exploits help to minimize user interaction and awareness when implanting RCS on a target device. We show evidence that a single commercial vendor may have supplied Hacking Team customers with exploits for at least the past two years, and consider this vendor's relationship with French exploit provider VUPEN.

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