Network Injection Appliances Used to Install Surveillance Implants

Toronto, Canada (August 15, 2014) - The Citizen Lab is pleased to announce the release of "Schrodinger's Cat Video and the Death of Clear-Text" by Senior Security Researcher and Technical Advisor Morgan Marquis-Boire.

While there has been much discussion about the use of software described as 'implants' or 'backdoors' to perform targeted surveillance, this report is about the less well understood method by which most targeted surveillance is delivered: network injection. Taking advantage of security flaws in major web presences (such as Google's 'YouTube' and Microsoft's 'Live'), vendors have started selling turnkey solutions that enable easy installation of targeted surveillance software at scale.

The report rovides a detailed analysis of two products sold for facilitating targeted surveillance known as network injection appliances. These products allow for the easy deployment of targeted surveillance implants and are being sold by commercial vendors to countries around the world. Compromising a target becomes as simple as waiting for the user to view unencrypted content on the Internet.

While the technology required to perform such attacks has been understood for some time, there is limited documentation of the operation of these attacks by state actors. This report provides details on the use of such surveillance solutions including how they are built, deployed, and operated.

The Washington Post published an accompanying piece to the report. View the report on the Washington Post's front page [see PDF and PDF].

Morgan Marquis-Boire also authored an op-ed, published in The Intercept, on the report's findings.

About Morgan Marquis-Boire:
Morgan Marquis-Boire is a Senior Researcher and Technical Advisor at the Citizen Lab at the Munk School of Global Affairs, University of Toronto. He is the Director of Security for First Look Media. Prior to this he worked on the security team at Google. He is a founding member of The Secure Domain Foundation, a non-profit, free, adversary intelligence group. He is a Special Advisor to the Electronic Frontier Foundation in San Francisco and an Advisor to the United Nations Inter-regional Crime and Justice Research Institute. In addition to this, he serves as a member of the Free Press Foundation security advisory board. A native of New Zealand, He was one of the original founders of the KiwiCON hacker conference. His research on surveillance and the digital targeting of activists and journalists has been featured in numerous print and online publications.

-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