Civil Society Organizations Face Onslaught of Persistent Computer Espionage Attacks

Toronto, Canada (November 11, 2014) - Civil society organizations (CSOs) that work to protect human rights and civil liberties around the world are being bombarded with the same persistent and disruptive targeted computer espionage attacks reportedly hitting industry and government. Unlike industry and government, however, civil society organizations have far fewer resources to deal with the problem and rarely receive the same attention as the former. These attacks on civil society raise major issues for the sustainable promotion of rights and democracy worldwide.

These and other findings are detailed in a major new report published today by the Citizen Lab, an interdisciplinary research laboratory based at the University of Toronto's Munk School of Global Affairs.

The report, entitled ***Communities @ Risk*: *Targeted Digital Threats against Civil Society***, involved 10 civil society groups that enrolled as study subjects over a period of four years. The Citizen Lab study sought to obtain greater visibility into an often overlooked digital risk environment affecting--whether they know it or not--many of society's most essential institutions. The participating CSOs shared emails and attachments suspected of containing malicious software, network traffic, and other data with Citizen Lab researchers, who undertook confidential, detailed analysis. Citizen Lab researchers also paid site visits to the participating CSOs, and interviewed them about their perceptions and the impacts of the digital attacks on their operations. Data from both the technical and contextual aspects of the research informs the report's main findings.

"The *Communities @ Risk* report represents a major systematic effort to identify the type of digital attacks vexing human rights and other civil society organizations," explains **Professor Ron Deibert**, Director of the Citizen Lab. "It is well known that computer espionage is a problem facing Fortune 500 companies and government agencies. Less well known and researched, however, are the ways in which these same type of attacks affect smaller organizations promoting human rights, freedom of speech, and access to information. We set out to fill this gap in knowledge."

Among the other main findings of *Communities @ Risk*, Citizen Lab researchers found that the technical sophistication of even the most successful attacks against CSOs tends to be low. Instead, attackers put more significant time and effort into crafting legitimate-looking email messages or other "lures" designed to bait targets into opening attachments or clicking on links (also known as social engineering). The content for these lures is often derived from information gathered from previous breaches of individuals in their organization or partners in their wider communities. Constant use of socially engineered attacks as bait erodes trust among those communities and creates disincentives around using the very communication technologies that are often seen as CSOs' greatest asset.

Over a four-year period, researchers watched as attackers modified their malicious software and other attack techniques based on the CSOs' choices of operating systems and other platforms, which indicates the persistent and evolving nature of targeted digital threats. The report also underscores the transnational dimension of targeted digital threats on CSOs. Targeted digital threats provide means for a powerful threat actor, such as a state, to extend its reach beyond borders and into "safe areas," monitoring exiled journalists, diaspora, and human rights groups as if they were within physical proximity.

The report argues that solving the problem will require major efforts among several stakeholders, from the foundations that fund civil society, to the private sector, to governments.

Funders are in a unique position to support grantees in making measurable improvements to their organizational security, but must first take steps to properly evaluate digital risks to both themselves and their grantees.

Companies that build software or provide information security have an *obligation* to support CSOs at risk, and the report recommends they explore a “pro bono” model of help as well as creative licensing solutions for CSOs to avoid the use of insecure, outdated software.

Finally, governments that support the right to privacy and freedom of expression online should take steps to raise the profile of targeted digital threats against civil society in their domestic policy and diplomacy, “treating the matter as of equal priority to their defense of the private sector.”

The full report, including detailed technical data related to *Communites @ Risk*, can be found at https://targetedthreats.net/

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. The Citizen Lab’s research on Targeted Digital Threats is supported by a grant from the John D. and Catherine T. MacArthur Foundation.

For more information, contact:
Irene Poetranto
Communications Officer
Citizen Lab
Munk School of Global Affairs, University of Toronto
Tel: 416-946-8903
irene.poetranto@utoronto.ca