UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

Mr. Adi Dar
Executive Vice President and General Manager
Cyberbit Ltd.
22 Zarhin St.
Ra'anana 4310602
Israel
Via E-Mail: Adi.dar@cyberbitc.com

November 29, 2017

Dear Mr. Dar:

Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto, researching information controls and their impact on human rights. We write regarding our research into the apparent use of Cyberbit's PC Surveillance System (PSS) by agencies of the Ethiopian government to target civil society in the United States and elsewhere, including an Oromo media outlet, a lawyer, and Citizen Lab's own research fellow Bill Marczak. This letter summarizes the main findings of our forthcoming research report, and raises questions to which we would appreciate your considered response. We will publish in full any statement or clarification you wish to provide. We plan on publishing our report no sooner than December 6, 2017.

Our report describes a campaign of targeted malware attacks, taking place from 2016 through the present, focused on individuals and issues associated with Ethiopia's Oromo ethnic group. Oromia is the largest regional ethnic state of Ethiopia, comprised mostly of the Oromo people. The Ethiopian government has targeted the Oromo people in a violent crackdown, beginning after Oromo peaceful protests in late 2015. The crackdown is estimated to have resulted in over 400 deaths. We obtained and analyzed commercial spyware targeting individuals associated with the Oromia Media Network, which is based in the United States and produces independent reporting regarding the Ethiopian state of Oromia; as well as a visiting academic fellow at Washington and Lee University School of Law in Virginia, who was the founder of the Association of Oromo Public Defenders (Public Interest Lawyers Association) in Oromia.

In the attacks documented in our report, targets received emails with content pertaining to Ethiopia and/or Oromo issues. The emails included a link to a malicious website impersonating an online Eritrean video portal. When a target clicks on the link, they are invited to download and install a real Adobe Flash update bundled with spyware from a page on getadobeplayer[.]com, before viewing the video. During the course of our research into the targets of this spyware campaign, Citizen Lab research fellow Bill Marczak was also targeted with a malicious email following this same pattern, after he corresponded with one of the targets whose Gmail account had been compromised.

By monitoring getadobeplayer[.]com, we found several samples of the spyware as it was updated over time. Each sample communicated with two command and control servers: time-local[.]com and time-local[.]net. We discovered that the spyware's command and control servers have public logfiles that appear to show both operator and victim activity, providing insight into the identity of the operators and the targets. Based on our analysis of the logfile, it appears that the spyware's operators are inside Ethiopia, and victims include Oromo activists as well as various Eritrean companies and government agencies. We observed what appear to be 43 successful infections.

We conducted scanning based on our fingerprinting of the two command and control servers, and found several other IP addresses matching that fingerprint. While monitoring the IP addresses matching our scan results, we noticed that the behavior of one of the IP addresses temporarily changed to return a directory listing in response to a normal GET / HTTP/1.1 request. That directory listing included the server hostname "cyberbitc.com," which was registered to Cyberbit. We also found a structurally similar sample in VirusTotal that dropped an EXE file signed by C4 Security, the entity that was the original developer of PSS, which was acquired by Elbit Systems in June 2011.

Of the IP addresses we found in our scanning, several of those appear to be demonstration servers used by Cyberbit, as their logfiles included the IP address 37.142.120.xxx, which is pointed to by a subdomain of cyberbit[.]net. The logfiles also indicate what appear to be recent demonstrations of the spyware to a number of governments and government agencies, including Uzbekistan's National Security Service, Zambia's Financial Intelligence Center, Kazakhstan, Vietnam, Nigeria, Rwanda, and the Philippine President's Malacañang Palace.

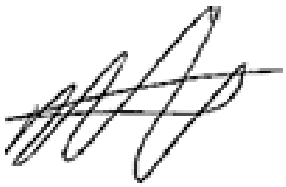
As you may be aware, and as the UN Guiding Principles on Business and Human Rights make clear, companies have an independent responsibility to respect human rights -- to avoid causing or contributing to adverse human rights impacts, and to address such impacts when they occur. Targeting of civil society -- journalists, researchers, lawyers, and others who are exercising the

rights to which they are entitled under international human rights law -- for digital espionage undermines their rights to privacy and freedom of opinion and expression, and presents additional concerns under applicable national laws. Our findings raise a number of questions surrounding Cyberbit's human rights due diligence practices and other internal processes to prevent and address adverse human rights impacts associated with its products and services:

1. Does Cyberbit sell its PSS product and associated services exclusively to law enforcement and intelligence agencies? If not, to what other entities does Cyberbit sell the PSS product?
2. Does Cyberbit provide training and/or ongoing support to clients regarding the use of its products?
3. Which export controls are applicable to Cyberbit's export of PSS? What internal procedures does Cyberbit maintain to ensure compliance with applicable export regulations? How many times has an export license been denied to Cyberbit for the export of PSS?
4. What policies and procedures does Cyberbit, or its parent company Elbit Systems, have in place concerning human rights and/or corporate social responsibility? Do Cyberbit employees receive any human rights-related training?
5. What if any due diligence does Cyberbit undertake concerning potential clients? Does it investigate a client's track record regarding human rights, or known incidents of spyware misuse by the client?
6. What steps does Cyberbit take when informed of an incident of misuse of its products?
7. Does Cyberbit monitor the manner in which its product is used by clients? Does Cyberbit monitor human rights- or conflict-related developments concerning a client?
8. How does Cyberbit ensure that its products are not used by clients in a manner that may violate civil or criminal laws (e.g., regarding wiretapping or computer fraud) in the jurisdiction where a target is located (e.g., the United States)?
9. Does Cyberbit include any provisions in its contracts concerning human rights or misuse of its product?
10. Has Cyberbit designed any of its products to spoof third-party software, such as Adobe Flash Player, in order to induce targets to launch the spyware?
11. How does Cyberbit obtain digital code-signing certificates for its spyware? Do third parties obtain such certificates on Cyberbit's behalf?
12. What action will Cyberbit take to address the misuse of its product to target Oromo activists?
13. What action will Cyberbit take to address the misuse of its product to target Citizen Lab research fellow Bill Marczak?

Your substantive response will provide a welcome example of transparency in an otherwise opaque market that has lent itself to significant abuses. Thank you in advance for your timely reply.

Sincerely,



Professor Ronald Deibert
Director, The Citizen Lab
Munk School of Global Affairs
University of Toronto

Cc: Sharon Rosenman
VP Marketing
Cyberbit Ltd.
E-Mail: sharon.rosenman@cyberbit.com

Dalia Rosen
VP, Head of Corporate Communications
Elbit Systems
E-mail: dalia.rosen@elbitsystems.com

Dana Tal-Noyman
Corporate Communications
Elbit Systems
E-Mail: dana.tal@elbitsystems.com