UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

Michael Dillon
Executive Vice President, General Counsel and Corporate Secretary
Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA

Via E-Mail: midillon@adobe.com

December 1, 2017

Dear Mr. Dillon,

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 recent discovery of the misuse of Adobe Flash Player software in advanced commercial spyware targeting journalists, lawyers, researchers, and others. This letter is to (a) alert you to the misuse of your product, and (b) seek information on the steps Adobe will take to address this misuse.

As you may be aware, Citizen Lab research has investigated the use of advanced commercial spyware against civil society actors for a number of years.[1] Our recent research concerns the apparent use of commercial spyware by agencies of the Ethiopian government to target civil society working on Oromo issues in the United States and elsewhere, including an Oromo media outlet, a lawyer who has worked on Oromo causes, and Citizen Lab's own research fellow Bill Marczak. 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, which began after Oromo peaceful protests in late 2015. The crackdown is estimated to have resulted in over 400 deaths.[2]

[1] Citizen Lab reports regarding commercial spyware are available at https://citizenlab.ca/category/research/targeted-threats/.
[2] Human Rights Watch, "'Such a Brutal Crackdown': Killings and Arrests in Response to Ethiopia's Oromo Protests," June 15, 2016, https://www.hrw.org/report/2016/06/15/such-brutal-crackdown/killings-and-arrests-response-ethiopias-oromo-protests.

In studying the operation of the spyware, we uncovered evidence that the spyware used is PC Surveillance System (PSS), a product offered to law enforcement and intelligence agencies by Cyberbit, a wholly-owned subsidiary of Elbit Systems. We observed that in order to infect a targeted machine, the spyware operator would send targets an email containing a link to a malicious website impersonating an online video portal. When a target clicks on the link, they are invited to download and install an Adobe Flash Player update that has been repackaged to contain the spyware before viewing the video. The following is one example of a malicious email we documented:

From: sbo radio <sbo.radio88@gmail.com>
Date: Tue, 4 Oct 2016 16:50:13 +0300
Subject: Fw: Confidential video made public

What do you think of this video ? In case you don't have the right version of adobe flash and can't watch the video, you can get the latest version of Adobe flash from Here
http://getadobeplayer[.]com/flashplayer/download/index7371.html.

---------- Forwarded message ----------
From: sbo radio <sbo.radio88@gmail.com>
Date: Tue, Oct 10, 2014 at 4:23 PM
Subject: Video hints Eritrea and Ethiopia war is highly likely to continue

Dear Excellencies,

Video : Eritrea and Ethiopia war likely to continue
http://www.eastafro[.]net/eritrea-ethiopia-border-clash-video.html

regards,

Sbo Radio
Mit freundlichen Grüßen

When a target clicks on an operator-generated link to eastafro[.]net, JavaScript on the site checks to see whether the target is using Windows, and whether their Adobe Flash Player is up to date. If the script detects a Windows user with an out-of-date Flash Player, it displays a message asking the user to update their Flash Player. If clicked, or after 15 seconds, the user is

redirected to a page on **getadobeplayer[.]com**, which offers the user a *real* Flash Player update bundled with spyware.

In another malicious email targeting an Oromo activist, the website link provided resulted in the following prompt: "Adobe's PdfWriter allows you to view PDF files easily from your browser," adjacent to an Adobe PDF logo. Clicking on the prompt would result in download of CutePDF Writer software bundled with the spyware.

It thus appears that this spyware is intended to prey on a user's trust in Adobe Systems, as well as user reliance on the Adobe Flash Player. The spyware incorporates the Adobe Flash Player software outright, and attempts to spoof legitimate Adobe resources through use of Adobe and Flash trademarks. While it is unknown whether Cyberbit made the design decision to spoof Adobe in its spyware, or whether the spyware operator incorporated that feature after obtaining PSS, it is clear that such spoofing techniques are frequently relied upon by advanced commercial spyware companies and others to ensure the effectiveness of a digital espionage operation. For example, commercial spyware produced by Gamma Group spoofed Mozilla Firefox in the past, prompting Mozilla to send the company a cease-and-desist letter.[3] Similarly, Russian threat actor APT28 has registered hundreds of domain names that incorporate Microsoft branding; that practice prompted Microsoft to file suit in US court against the malware operators in order to seize and sinkhole the domains, successfully.[4]

In sum, we have uncovered evidence that the Ethiopian government is using Cyberbit's PSS spyware, masquerading as Adobe products, to target dissidents in the United States and elsewhere. This activity is in contravention of the rights to privacy and freedom of opinion and expression under international human rights law, and raises a number of concerns under US law (including criminal law provisions related to computer fraud and abuse and interception of private communications, as well as intellectual property law concerns). This activity undermines not only the human rights of those targeted, but also the security of the digital ecosystem as a whole, and user confidence in Adobe software in particular.

We would appreciate if you could inform us whether Adobe Systems will take any action regarding the incorporation of Adobe Flash Player and Adobe trademarks in the targeted spyware attacks we have outlined herein. We plan to publish a report on our findings on

[3] Alex Fowler, "Protecting our brand from a global spyware provider," Mozilla Blog, April 30, 2013, https://blog.mozilla.org/blog/2013/04/30/protecting-our-brand-from-a-global-spyware-provider/.
[4] Kevin Poulsen, "Putin's Hackers Now Under Attack—From Microsoft," Daily Beast, July 20, 2017, https://www.thedailybeast.com/microsoft-pushes-to-take-over-russian-spies-network; see also the Microsoft pleading documents available at https://www.noticeofpleadings.com/strontium/.

December 6, 2017. We are happy to include with that report any response you wish to make public.

Please let us know if we can provide you with any additional information. Thank you for your prompt attention to this matter.

Sincerely,

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