



March 1, 2018

Dear Mr. Cantor and Mr. Kowal:

Citizen Lab is in receipt of correspondence from Mr. Cantor dated February 16, 2018 and Mr. Kowal dated February 20, 2018.

As you know, upon receipt of Sandvine's letter, Citizen Lab deferred publication of its report concerning Sandvine's PacketLogic Devices (the "Report") in order:

- to investigate further Sandvine's assertions; and
- to conduct additional due diligence into the research process, methodology, and conclusions in the Report.

This process included Citizen Lab arranging for two confidential, independent, third-party peer reviews of the Report.

These additional steps confirmed the thoroughness of the research process and methodology employed, as well as the reasonableness and accuracy of the conclusions in the Report.

To be clear, in the Report, Citizen Lab does not suggest that PacketLogic devices are capable of injecting traffic with the malicious code outright. Rather, as noted in our initial communication to you, the spyware injection and advertising injection was carried out by injecting HTTP 307 redirects which caused a target's browser to automatically fetch malicious code from a separate website. The injection of various HTTP redirects is an established spyware and advertising injection technique. For instance, a 2010 patent application from Hacking Team entitled "Method and Device for Network Traffic Manipulation" describes [injecting an HTTP 302 redirect](#) that causes a target's web browser to fetch a malicious file as a way to inject spyware. The NSA's QUANTUM system for spyware injection is also [believed to function](#) by injecting HTTP redirects. A study published in the Proceedings of the 25th USENIX Security Symposium in August 2016 found what appeared to be several groups injecting HTTP redirects to send users to malware or advertisements.

In your February 16, 2018 letter, Sandvine states both that PacketLogic is "not capable of any form of payload injection," and that the design "does not permit the end user to



inject a payload larger than 1 packet”. This latter assertion, indicating an injection of one packet is possible, is consistent with Citizen Lab’s findings.

Neither in the Report nor in our correspondence to you does Citizen Lab suggest that Sandvine has a “commercial or technology relationship with FinFisher or any surveillance technology vendors.” However, the evidence does suggest Sandvine’s PacketLogic is used by government-linked operators to employ injection capabilities according to their preference — whether that be through use of FinFisher or some other malicious code. The point is not that Sandvine was directly involved in that selection but, rather, that Sandvine’s product can be and, in fact, appears to have been used in this manner. This, in turn, engages issues of Sandvine’s corporate social responsibility, and that of Francisco Partners, all of which is a matter of important public interest and discussion.

Mr. Cantor has provided information regarding Sandvine’s “Comprehensive Business Ethics Program.” We have a number of important follow up questions below. Citizen Lab will include the details you have provided and your response, if any, to these follow-up questions in its forthcoming Report:

- Given the apparent use of PacketLogic technology in Turkey and Egypt in a manner that violates Sandvine’s end user license agreement, ethics policies, and Business Ethics Committee standards, does Sandvine intend to terminate offending deployments?
- Does Sandvine intend to address the misuse documented by Citizen Lab in any other way?
- Has the Sandvine Business Ethics Committee convened to discuss the use of its products in Turkey and/or Egypt? If so, what was the result? If not, will it do so in a timely fashion?
- Has the Sandvine Business Ethics Committee convened to discuss the Citizen Lab findings? If so, what was the result? If not, will it do so in a timely fashion?
- Your website reflects that the Sandvine Business Ethics Committee (BEC) must approve sales to “any country not rated an ‘A’ by the World Bank,” and obtain a signed certificate of compliance from the customer. It further notes that “Sandvine employees and partners are prohibited from selling solutions to countries that are embargoed or sanctioned by the EU, US, and/or UN are rated



UNIVERSITY OF
TORONTO

MUNK
SCHOOL
OF
GLOBAL
AFFAIRS

Join the Global Conversation

a 'D'." To what specific grading mechanism do these statements refer? It appears your policy draws on the Worldwide Governance Indicators (WGI). However, it is unclear how letter grades are determined or from where they originate. Can you provide more detail regarding this process? We note that the WGI 2016 percentile scores for Turkey and Egypt on the indicators specified in your policy are quite low; at what percentile do sales require BEC approval?

For Francisco Partners, Mr. Kowal has indicated his willingness to engage in a dialogue on corporate governance, but has not responded to all of the specific questions in our letter.

In keeping with Citizen Lab's approach to transparent and fair publication, we are again providing Sandvine and Francisco Partners an opportunity to respond to Citizen Lab's research findings and questions before releasing the Report.

Citizen Lab plans to publish its final report on Thursday March 8, 2018. We welcome your response to the follow-up questions before then.

In short, Citizen Lab is confident in the veracity of its research findings and the reasonableness of its conclusions and is committed to public transparency on this important issue of public interest.

Finally, we strongly disagree with Sandvine's allegations concerning Citizen Lab's acquisition and use of the PacketLogic device. Please provide us with the full factual basis for these allegations so we may provide an informed response.

Sincerely,

Professor Ronald J. Deibert Professor Political Science Department Director, Citizen Lab at the Munk School of Global Affairs University of Toronto

At Trinity College
1 Devonshire Place, Toronto, ON
Canada M5S 3K7
T: 416-946-8900 F: 416-946-8915

At the Observatory
315 Bloor Street West, Toronto, ON
Canada M5S 0A3
T: 416-946-8929 F: 416-946-8877

www.munkschool.utoronto.ca