UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

Andrew Kowal
Deal Partner, Francisco Partners
One Letterman Drive
Building C - Suite 410
San Francisco, CA 94129
Via e-mail: Kowal@franciscopartners.com

Brian Decker
Deal Partner, Francisco Partners
One Letterman Drive
Building C - Suite 410
San Francisco, CA 94129
Via e-mail: decker@franciscopartners.com

Lyndon Cantor
Chief Executive Officer, Sandvine
Operating Partner, Francisco Partners Consulting
One Letterman Drive
Building C - Suite 410
San Francisco, CA 94129
Via e-mail: Cantor@franciscopartners.com

February 12, 2018

Dear Mr. Kowal, Mr. Decker, and Mr. Cantor:

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 understand you are each part of the Francisco Partners' team responsible for the firm's investment in Procera Networks, as well as current members of the board of directors of Sandvine, with which Procera Networks merged in 2017. Accordingly, we write to you regarding our research into the apparent use of Procera Networks/Sandvine PacketLogic devices by entities within Turkey and Egypt to engage in malicious network injection.

In the case of Turkey, PacketLogic devices were used to inject traffic on dozens of targeted IP addresses with spyware, in at least five provinces. In addition to targets in Turkey, targets included some users physically located in Syria -- a country subject to U.S. and Canadian sanctions -- who used Internet

services beamed into Syria by Turk Telecom subscribers via cross-border directional Wi-Fi links. In the case of Egypt, PacketLogic devices were used to inject traffic on a mass scale with advertisements and browser cryptocurrency mining scripts, apparently for profit. These uses of the PacketLogic product present serious human rights and corporate social responsibility concerns.

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 February 20, 2018.

As you know, in October 2016 the media reported on the involvement of Procera Networks in equipping the Turkish government with a deep packet inspection (DPI) system, allegedly used to surveil the population.[1] Almost a year later, security company ESET reported it had observed Internet Service Providers (ISPs) in two countries tampering with some of their users' internet activity.[2] When these users attempted to download certain legitimate programs, the ISPs caused them instead to download programs that were bundled with FinFisher, a government-exclusive spyware program. Injecting their downloads with malware enabled the surreptitious infection and monitoring of these individuals. ESET did not release the names of the countries or ISPs investigated. Citizen Lab's current research investigation, however, confirms that the network injection reported on by ESET was undertaken in Turkey and Egypt, using DPI technology built by Procera Networks, now Sandvine.

Our research report describes how we used Internet scanning to localize the network injection reported on by ESET, and traced it to Turkey and Egypt. We found several middleboxes on Turk Telecom's backbone network redirecting a small number of users who attempt to download legitimate software (including Opera, Avast Antivirus, and CCleaner) to malicious versions. The malicious versions include spyware that appears to be of the same type as was used in the *StrongPity APT* attacks.[3] We also found a similar middlebox at a cable landing station in Egypt that is injecting ads and browser cryptocurrency mining scripts. The same devices in both Turkey and Egypt are additionally blocking political and human rights content by injecting TCP reset packets. We matched characteristics of the network injection to a second-hand PacketLogic device that we purchased, as well as the PacketLogic client software. Packets injected by the middleboxes we identified in Turkey and Egypt have the same distinctive value in their IP identification field (0x3412) as our PacketLogic device. The HTTP redirects inside the injected packets we

[1] https://www.forbes.com/sites/thomasbrewster/2016/10/25/procera-francisco-partners-turkey-surveillance-erdogan

[2] https://www.welivesecurity.com/2017/09/21/new-finfisher-surveillance-campaigns/

[3] https://securelist.com/on-the-strongpity-waterhole-attacks-targeting-italian-and-belgian-encryption-users/76147/

identified in Turkey and Egypt exactly match the form of HTTP 307 redirects inserted by the PacketLogic client software when an operator clicks the "Insert 307 Temporary Redirect" button in the interface. These findings are a strong indication that entities with access to ISP networks in Turkey and Egypt have employed Sandvine's PacketLogic technology to target users for surveillance, engage in censorship, and compromise users' digital security for profit.

We note that Francisco Partners has a track record of investing in companies that provide dual-use technologies with security and human rights implications. These companies include NSO Group, Blue Coat, and Procera Networks, among others. It appears that Francisco Partners has determined that targeting the cybersecurity sector in particular for investment is a profitable enterprise. Yet it is unclear whether the firm has evaluated the particular rights-related risks inherent in that sector, as Francisco Partners has issued no statements on corporate social responsibility. Additionally, we are concerned over reporting that, with respect to Turkey, "the acquisition [of Procera Networks] by Francisco Partners led to greater focus on 'regulatory compliance... mostly bulk surveillance.' Another [Procera employee] claimed: 'When Francisco Partners took control it was business ethics that mattered, not human ethics.'"[4]

This situation raises a few questions surrounding Francisco Partners' knowledge of and role in the Turkey and Egypt deployments of PacketLogic:

1. How has Francisco Partners directed or influenced the business strategy of Procera Networks/Sandvine?
2. Did Francisco Partners provide any input on the sales or deployment of PacketLogic in Turkey or Egypt? How did it respond to the concerns reportedly raised by Procera Networks employees in 2016 regarding the use of Procera technology to conduct surveillance in Turkey?
3. Does Francisco Partners provide the companies in which it invests, including Procera Networks/Sandvine, with any guidance concerning due diligence, human rights, or corporate social responsibility?
4. What are Francisco Partners' own internal policies or practices concerning human rights and corporate social responsibility?
5. Was Francisco Partners aware of the use by Procera Networks/Sandvine of deep packet inspection (DPI) technology to offer network injection capabilities?
6. Will Francisco Partners address the use of Sandvine technology for spyware injection in Turkey and Syria, and for mass advertising injection in Egypt?

[4] https://www.forbes.com/sites/thomasbrewster/2016/10/25/procera-francisco-partners-turkey-surveillance-erdogan

Finally, in light of Francisco Partners' history of funding technology companies that present significant human rights concerns, we strongly encourage you to open a dialogue with civil society (NGOs, activists, academics, country experts, etc.) to obtain input on how your firm might encourage greater respect for human rights by the businesses in which it invests. Indeed, socially responsible investment is both a catalyst for progress in human rights, and an emerging expectation for the private sector. You may be aware that BlackRock Chairman and CEO Larry Fink recently issued a letter to CEOs,[5] noting:

> Society is demanding that companies, both public and private, serve a social purpose. To prosper over time, every company must not only deliver financial performance, but also show how it makes a positive contribution to society. Companies must benefit *all of their stakeholders*, including shareholders, employees, customers, *and the communities in which they operate* (emphasis added).

This call echoes aspects of the UN Guiding Principles on Business and Human Rights,[6] which make clear that all 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. Will Francisco Partners take this opportunity to review its own role in setting the rights-related impacts deemed acceptable amongst advanced technology companies?

Thank you in advance for your timely reply. For your information, we have also sent a separate letter to Mr. Cantor and Mr. Alexander Havänig, as executive leadership at Sandvine, describing our upcoming report and presenting a series of questions for comment.

Sincerely,

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

[5] https://www.blackrock.com/corporate/en-no/investor-relations/larry-fink-ceo-letter

[6] http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

Cc: Dipanjan Deb
Co-Founder and Chief Executive Officer, Francisco Partners
deb@franciscopartners.com

info@franciscopartners.com

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