UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

Lyndon Cantor
Chief Executive Officer, Sandvine
Operating Partner, Francisco Partners Consulting
Via e-mail: lyn.cantor@sandvine.com
Cantor@franciscopartners.com

Alexander Haväng
Chief Technical Officer, Sandvine
Via e-mail: info@sandvine.com

February 12, 2018

Dear Mr. Cantor and Mr. Haväng:

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 Sandvine's 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 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

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

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 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.

While researchers and others have hypothesized that network injection techniques could at some point be deployed by a nation-state to surreptitiously infect targets with malware, the apparent use of your PacketLogic product in Turkey to do so is, to our knowledge, the first publicly documented instance. Such deployment is unusual, perhaps because of the sheer brazenness involved, as well as the significant legal, ethical, and political lines crossed. By way of comparison, other digiourtal intrusions known to rely on network injection include the U.S. National Security Agency's QUANTUM program as described in leaked NSA documents;[4] and China's "Great Cannon," which injected JavaScript to enlist

[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/

[4] https://www.wired.com/2015/04/researchers-uncover-method-detect-nsa-quantum-insert-hacks/

targets' browsers in DDoS attacks against politically sensitive overseas websites, in what amounted to an extraterritorial act of political retaliation.[5] Network injection is particularly egregious because it employs a man-in-the-middle technique that typically relies on tampering by Internet Service Providers (ISPs) with some of their users' Internet traffic. The abuse of an ISP's trusted position on the network to actually inject malware into its customers' traffic raises serious questions under domestic and international law, including with respect to the right to privacy under international human rights law. Meanwhile, the use of network injection in Egypt to serve ads and browser cryptocurrency mining scripts for profit is a clear sign of the abuse potential and lack of oversight associated with such an intrusive technique.

As you may be aware, and as the UN Guiding Principles on Business and Human Rights[6] 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.

Our findings raise a number of questions surrounding Sandvine'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. Since the October 2016 media reporting, has Procera Networks or Sandvine taken any steps to address the human rights concerns raised by their employees with respect to Turkey? If so, what steps?
2. What is the current status of the ethics committee reportedly[7] established by Procera? Post-merger, does Sandvine maintain an ethics committee or engage in ethics reviews? If so, what issues were raised in ethics reviews of business in Turkey and Egypt?
3. What if any other human rights due diligence or corporate social responsibility policies or practices are in place at Sandvine?
4. Does Sandvine maintain a resident solutions engineer or other customer support staff in Turkey or in Egypt? If so, what is the scope of work of such person(s)?
5. Does Sandvine monitor in any way the use of network injection techniques provided through its PacketLogic devices?
6. Was Sandvine aware of the use of PacketLogic technology in Turkey to inject spyware in network traffic?

[5] https://citizenlab.ca/2015/04/chinas-great-cannon/

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

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

7. Was Sandvine aware of the use of PacketLogic technology in Egypt for mass connection hijacking to deliver affiliate ads?
8. How will Sandvine address the use of its PacketLogic product in Turkey to inject spyware?
9. How will Sandvine address the use of its PacketLogic product on network traffic in Syria, a country subject to U.S. and Canadian sanctions?
10. How will Sandvine address the use of its PacketLogic product in Egypt for mass connection hijacking to deliver affiliate ads?
11. Will Sandvine modify in any way the network injection capabilities provided through its products and services, given the abuses documented?

Thank you in advance for your timely reply.

Sincerely,

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