Citizen Lab Report – Omar Abdulaziz / Pegasus Spyware

Background:

Between October 1 and 2, 2018, a number of media outlets published articles about Omar Abdulaziz. Mr. Abdulaziz is a Saudi national with Permanent Resident status in Canada who has been a vocal online critic of the Saudi Government and its human rights record. The media articles were based on a report published by the Citizen Lab at the University of Toronto on September 18, 2018, entitled Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. The Citizen Lab report alleges that Pegasus spyware has been used by a number of governments with questionable human rights records, including Saudi Arabia, to surveil human rights activists and other civil society groups. The report also indicates that one or more of the targets infected with Pegasus may have been in Canada. Citizen Lab subsequently met with Mr. Abdulaziz, inspected his iPhone and confirmed that it had in fact been infected with Pegasus spyware.

Pegasus is sold by NSO Group, a privately-held cyber intelligence company based in Herzliya, Israel. The NSO Group states that it provides "authorized governments with technology that helps them combat terror and crime." The fact that Pegasus is meant to be sold exclusively to government departments and agencies elevates this alleged hack from a cybercrime incident to a potential act of foreign interference. This is not a tool that commercial hackers would normally have access to.

Pegasus spyware is designed to be covertly installed on Apple or Android smartphones. Once in place, it exploits vulnerabilities in the phone's operating system to give the hacker access to text messages, track phone calls, collect passwords, tracing the location of the phone, and gather information from installed applications, and from the phone's cameras and microphones.

A statement released by NSO Group in response to the report indicated that the company works in full compliance with all applicable laws, including export control laws. NSO Group argued that there were a number of inaccuracies in the Citizen Lab report, including the list of countries in which the NSO operates.

The Criminal Code has prohibitions against the unauthorized use of a computer system and mischief to data. If Pegasus was used to hack cellphones in Canada, the RCMP can investigate.

The RCMP is closely examining the Citizen Lab report. Recognizing the importance of enhancing operational capacity in advance of the 2019 Federal Election, the RCMP is establishing a foreign interference team to disrupt and investigate threats to the democratic and electoral processes.

Contacts:
Prepared by: Alison Whelan, Executive Director, Federal Policing Strategic Direction, 613-843-4494
Approved by: Gilles Michaud, Deputy Commissioner, Federal Policing, 613-843-4494

Pages 36 to / à 37

are not relevant

sont non pertinentes

CITIZEN LAB REPORT – PEGASUS SPYWARE

- The Government of Canada's top priority is ensuring the safety and security of citizens and safeguarding their privacy.
- The Government is aware of the Citizen Lab report and the related media reporting. The allegations the privacy of at least one individual may have been breached are deeply troubling.
- The Criminal Code has provisions against the unauthorized use of a computer system and mischief to data. Hacking or any other unwarranted intrusions into Canadian computers and mobile devices is a criminal act.
- The matter is currently being reviewed by the RCMP.

Page 39

is not relevant

est non pertinente

BACKGROUND

- Between October 1-2, 2018, a number of media outlets published articles about Omar Abdulaziz. Mr. Abdulaziz is a Saudi national with Permanent Resident status in Canada who has been a vocal online critic of the Saudi Government and its human rights record. The media articles were based on a report published by the Citizen Lab at the University of Toronto on September 18, 2018 entitled Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. The Citizen Lab report alleges that Pegasus spyware has been used by a number of governments with questionable human rights records, including Saudi Arabia, to surveil human rights activists and other civil society groups. The report also indicates that one or more of the targets infected with Pegasus may have been in Canada. Citizen Lab subsequently met with Mr. Abdulaziz, inspected his iPhone and confirmed that it had in fact been infected with Pegasus spyware.

- Pegasus is sold by NSO Group, a privately-held cyber intelligence company based in Herzliya, Israel. The NSO Group states that it provides "authorized governments with technology that helps them combat terror and crime." The fact that Pegasus is meant to be sold exclusively to government departments and agencies elevates this alleged hack from a cybercrime incident to a potential act of foreign interference. This is not a tool that commercial hackers would normally have access to.

- Pegasus spyware is designed to be covertly installed on Apple or Android smartphones. Once in place, it exploits vulnerabilities in the phone's operating system to give the hacker access to text messages, track phone calls, collect passwords, tracing the location of the phone, and gather information from installed applications, and from the phone's cameras and microphones.

- A statement released by NSO Group in response to the report indicated that the company works in full compliance with all applicable laws, including export control laws. NSO Group argued that there were a number of inaccuracies in the Citizen Lab report, including the list of countries in which the NSO operates.

- The Criminal Code has prohibitions against the unauthorized use of a computer system and mischief to data. If Pegasus was used to hack cellphones in Canada, the RCMP can investigate. However, the ability of Canadian law enforcement to lay charges may be limited if the hacker was working from outside of Canada.

- The RCMP is closely examining the Citizen Lab report. Recognizing the importance of enhancing operational capacity in advance of the 2019 Federal Election, the RCMP is establishing a foreign interference team to disrupt and investigate threats to the democratic and electoral processes.

Name of PCO Policy Analyst. Nom de l'analyste du BCP :

Secretariat. Secrétariat :

Telephone number. Numéro de téléphone :

10/10/2019 3:21 PM

THREAT ASSESSMENT
SPECIAL EVENT

ITAC CIET
Integrated Terrorism Assessment Centre 2004 2019 Centre intégré d'évaluation du terrorisme

TA 19/101-A // 2019-09-06

UNCLASSIFIED//FOR OFFICIAL USE ONLY

43rd Canadian General Federal Election 2019

TERRORISM THREAT LEVELS

CANADA ↔ MEDIUM

LEGEND: Established ↔ Raised ↑ Lowered ↓ Remains ↔

INTRODUCTION

In accordance with procedures outlined in the Canada Elections Act regarding fixed dates, the 43rd Canadian General Election is scheduled to take place on or before 21 October 2019.

Source: Elections Canada Facebook

ASSESSMENT

-
-
-
-
-
-

ASSESSMENT NOTE

This report is based on open-source reporting

***DEFINITIONS** and **HANDLING INSTRUCTIONS** are located at the last page.*

Canada