THE KINGDOM CAME TO CANADA

How Saudi-Linked Digital Espionage Reached Canadian Soil

By Bill Marczak, John Scott-Railton, Adam Senft, Bahr Abdul Razzak, and Ron Deibert

OCTOBER 1, 2018
RESEARCH REPORT #115

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

THECITIZENLAB

Copyright

Suggested Citation

Bill Marczak, John Scott-Railton, Adam Senft , Bahr Abdul Razzak, and Ron Deibert. "The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil," Citizen Lab Research Report No. 115, University of Toronto, October 2018.

Acknowledgements

We thank Omar Abdulaziz for assisting with the investigation and consenting to the publication of this research. Being the victim of targeted digital espionage can be stigmatizing and we recognize his personal bravery for agreeing to be named.

Bill Marczak's work on this project was supported by the Center for Long Term Cybersecurity (CLTC) at UC Berkeley. This work was also supported by grants to the Citizen Lab from the Ford Foundation, the John T. and Catherine D. MacArthur Foundation, the Oak Foundation, the Open Society Foundations, and the Sigrid Rausing Trust.

Thanks to Brendan de Caires from PEN Canada and Brandon Silver and Professor Irwin Cotler from the Raoul Wallenberg Centre for Human Rights.

Editing and other assistance provided by Siena Anstis, Miles Kenyon, Cynthia Khoo, Masashi Crete-Nishihata, Jon Penney, and Mari Zhou.

Thanks to the University of Toronto's Research Ethics Board, and in particular Dr. Dean Sharpe.

About the Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a "mixed methods" approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

Contents

Key Findings

- **We have high confidence that the cellphone of Omar Abdulaziz, a Saudi activist and Canadian permanent resident, was targeted and infected with NSO Group's Pegasus spyware. Abdulaziz has been outspoken on an ongoing diplomatic feud over human rights issues between Canada and Saudi Arabia. The targeting occurred while Abdulaziz, who received asylum in Canada, was attending university in Quebec.**
- **During our recently published global mapping of NSO's Pegasus infrastructure, we identified a suspected infection located in Quebec, Canada, operated by what we infer is a Saudi Arabia-linked Pegasus operator. We matched the infection's pattern of life to the movements of Abdulaziz, and his phone, with his assistance. After examining his text messages, we identified a text message that masqueraded as a package tracking link. This message contained a link to a known Pegasus exploit domain.**
- **We are unaware of any legal authorization for the infection and monitoring of Omar Abdulaziz in Canada by a foreign government. If not properly authorized, the operators behind this targeting may have committed multiple Criminal Code offences, including willfully intercepting private communications contrary to section 184(1).**

1. Summary

Israel-based "Cyber Warfare" vendor NSO Group produces and sells Pegasus mobile phone spyware suite. Pegasus customers can infect targets using Androids and iPhones by sending them specially crafted exploit links. Once a phone is infected, the customer has full access to a victim's personal files, such as chats, emails, and photos. They can even surreptitiously use the phone's microphones and cameras to view and eavesdrop on their targets.

Over the past two years, multiple reports have emerged showing how Pegasus was abused by multiple NSO Group customers to target civil society. In 2016, Citizen Lab published the first report on the use of Pegasus, Million Dollar Dissident, which detailed how award-winning human rights defender Ahmed Mansoor was targeted, likely by the government of the United Arab Emirates. In 2017, Citizen Lab reported abusive uses of Pegasus spyware in Mexico, where targets included

lawyers, journalists, and politicians. In August 2018, Amnesty International reported that a Saudi dissident based abroad (later revealed to be Yahya Assiri), as well as an Amnesty researcher, were targeted with Pegasus. In addition, former president Ricardo Martinelli stands accused by the government of Panama of having used Pegasus during his tenure between 2009 and 2014 to systematically spy on political opponents and journalists.

In a September 2018 report titled Hide and Seek, we detailed our investigation into the global proliferation of Pegasus operators and infections. After scanning the Internet for Pegasus servers and grouping the 1,091 servers we found into 36 distinct operators, we used DNS cache probing to query Internet Service Providers (ISPs) around the world and identified 120 ISPs in 45 countries where we suspected Pegasus infections were located (**Figure 1**). Our technique was based on the assumption that Pegasus infections regularly "phone home" to their command and control (C&C) servers to exfiltrate information and receive new commands from their operator.

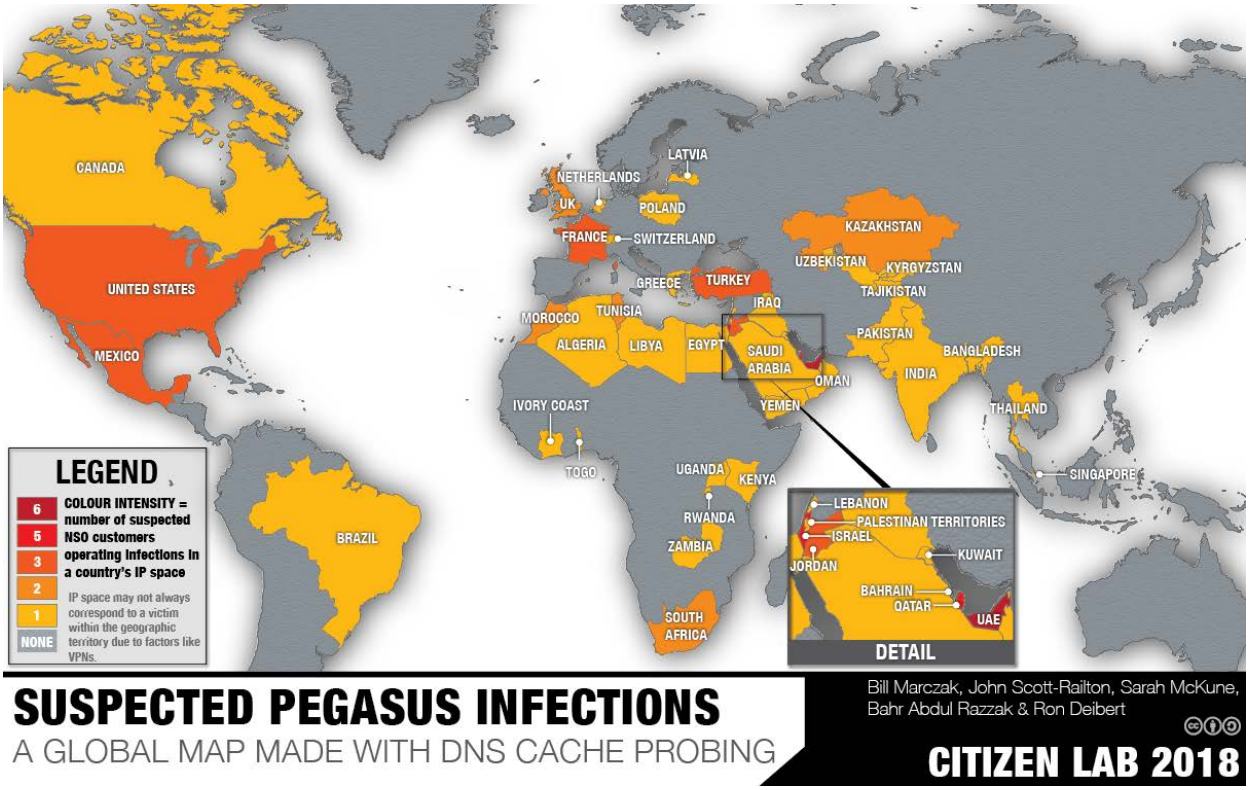

Figure 1: Global map of suspected NSO Pegasus infections.

Our *Hide and Seek* investigation revealed an intriguing suspected infection in Quebec, Canada. We observed the infection moving between a consumer ISP and a university ISP, during the evenings and outside of the academic year. We linked this infection to an operator that we call *KINGDOM*, which was also responsible for

the 2018 targeting of Saudi dissident Yahya Assiri and an Amnesty International researcher. Suspecting that the Canadian target was a Saudi-linked individual in Quebec, we contacted local members of the Saudi diaspora and attempted to identify a person whose movements fit the infection's pattern. We found one match: Omar Abdulaziz, a university student with a regular pattern of evening activity. On two specific days, we were able to match the timing of his evening activity, and then his return home, to the movement of the infection between the two ISPs. We also examined Abdulaziz's phone and found a fake package tracking notification SMS containing a Pegasus exploit link. These factors lead us to conclude with high confidence that Abdulaziz's iPhone was infected with NSO Group's Pegasus spyware.

Figure 2: Suspected infections operated by the KINGDOM NSO Group customer.

Abdulaziz is a Canadian permanent resident and vocal critic of the Saudi government. In 2014, he was forced to seek asylum in Canada in the face of strong pressure from the Saudi government. Today, Abdulaziz is a university student in Quebec, where he continues to be an outspoken voice on human rights issues in Saudi Arabia. In August 2018, Saudi authorities threatened his brother with jail time in what Abdulaziz believes was an attempt to pressure him into silence. When he continued speaking out, two of his brothers and several of his friends in Saudi Arabia disappeared. Pegasus would have allowed the operators to copy Abdulaziz's contacts, private family photos, text messages, and live voice calls from popular mobile messaging

apps. The operators could have even activated his phone's camera and microphone to capture activity, such as conversations, taking place in his home.

We are unaware of any legal authorization for the hacking and monitoring of Omar Abdulaziz in Canada by a foreign government. These actions may be contrary to multiple Criminal Code provisions, including willfully intercepting private communications, an indictable offence under section 184.

2. Omar Abdulaziz Targeted with Pegasus

Omar Abdulaziz is a prominent Saudi political activist who has been based in Canada since 2009. As a student at McGill University, Abdulaziz started a popular satirical news show on YouTube (Figure 3), which is highly critical of the Saudi government's repressive tactics and human rights record. The show has garnered millions of views, and he has developed a large social media following. After the Saudi government withdrew his scholarship to study in Canada, Abdulaziz applied for asylum and was granted permanent resident status in Canada in 2014.

Figure 3: A screenshot of Omar's Fitnah Show on YouTube.

Abdulaziz continues to be outspoken about the Saudi government's human rights record and has been particularly vocal and active during an ongoing diplomatic dispute between Canada and Saudi Arabia (See section 5), helping fellow Saudi students impacted by the dispute to claim asylum in Canada. Abdulaziz regularly appears in Canadian media, including a recent guest appearance on the Canadian Broadcasting Corporation (CBC)'s current affairs show, *The Current*, on August 10, 2018, where he said that Saudi authorities had entered his brother's home in Saudi

Arabia and "asked him to convince me [to] stop tweeting about what's really going on between Canada and Saudi Arabia, or they're going to send him to jail." The Saudi government appears to have made good on the threat: later in August, Abdulaziz's two brothers and a number of friends were arrested in Saudi Arabia. He believes that the arrests were an attempt to discourage him from speaking out further.

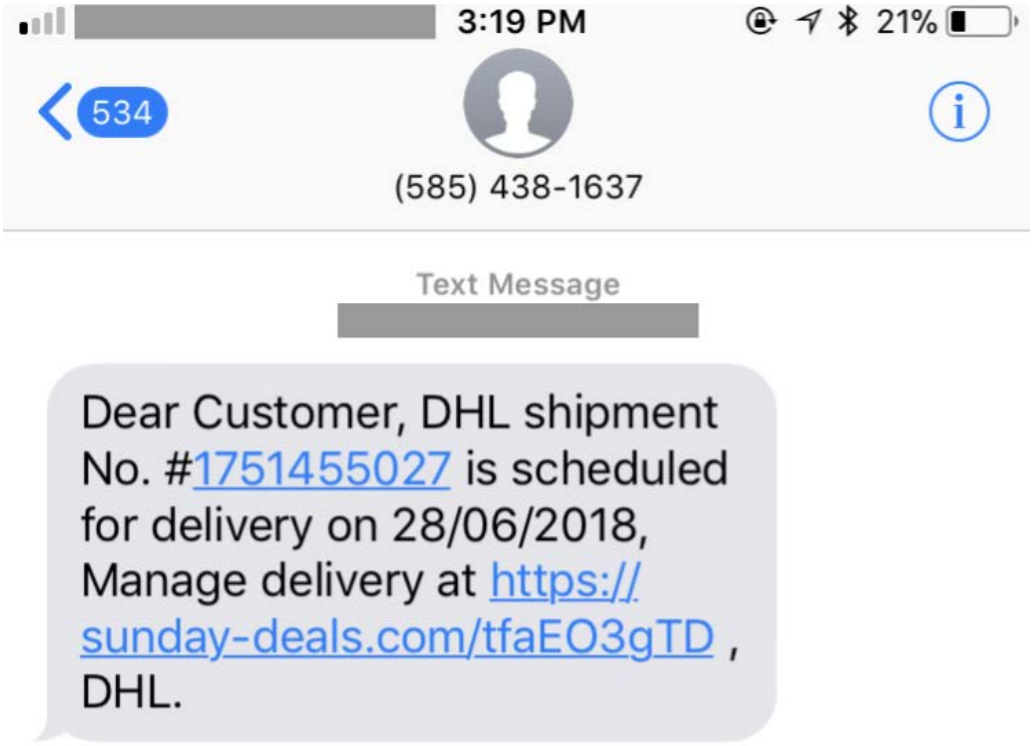

Figure 4. The SMS we found on Abdulaziz's phone, containing a link to an NSO Group exploit domain.

On a summer morning in 2018, Abdulaziz made a purchase on the online shopping website Amazon. Later that day he received a text message (Figure 4) purporting be a package shipment notification from the logistics company DHL. The URL in the message was from the domain **sunday-deals[.]com**. This domain belongs to a cluster that we previously identified as Pegasus exploit domains. Based on our prior research, we have high confidence that clicking on the link would result in the infection of the device with NSO's Pegasus spyware. Abdulaziz, who says he uses a separate phone for his activism, told us that the message arrived on his personal phone. Abdulaziz recalled thinking that the message was related to his online shopping.

We first contacted and obtained the SMS (Figure 4) from Abdulaziz following an extensive global study of suspected Pegasus infections (Section 3), which identified an interesting Saudi-linked infection in Quebec.

3. DNS Cache Probing Leads us to Abdulaziz

On September 18, 2018, we published a report titled Hide and Seek, which describes how we scanned the Internet to generate a list of Pegasus spyware servers, used a technique that we call ***Athena*** to group the servers into 36 distinct Pegasus systems, and performed DNS cache probing of ISPs to identify locations from where suspected Pegasus infections were phoning home. In total, we identified 120 ISPs in 45 countries with likely infections (Figure 1) and 10 Pegasus systems whose operators were engaging in suspected *cross-border monitoring* (i.e., monitoring infected devices in more than one country).

One of the Pegasus operators that appeared to be performing extensive cross-border operations was an operator we call *KINGDOM*. The KINGDOM operator appeared to be operating in the interests of Saudi Arabia, as it was the same operator that targeted London-based Saudi dissident Yahya Assiri and an Amnesty International researcher. In addition to suspected infections in Saudi Arabia, KINGDOM appeared to be actively monitoring targets in Bahrain, Canada, Egypt, France, Iraq, Jordan, Lebanon, Morocco, Qatar, Turkey and the UK.

A particularly interesting suspected KINGDOM infection was located in Quebec, Canada where we observed what appeared to be a single infected device moving between two different ISPs: a consumer ISP called Vidéotron and an academic ISP used by universities across Quebec called RISQ (Réseau d'informations scientifiques du Québec). The movement between Vidéotron and RISQ networks was distinctive because it occurred in the evenings and during the summer rather than the academic year.

Because the Quebec infection's operator was Saudi-linked, we suspected the victim was Saudi-linked as well. We reached out to members of the Saudi diaspora in Quebec and attempted to identify a person whose behaviour fit the pattern that we observed in the network traffic. We found one match: Omar Abdulaziz, a university student in Quebec. During the time that we monitored the infection, Abdulaziz moved between his apartment and an evening activity on his university's campus. Abdulaziz's home wifi is provided by Vidéotron and the university building where he engages in the evening evening activity offers wifi on the RISQ network. Abdulaziz regularly connected his iPhone to wifi in both locations. On two specific days, we were able to match the timing of his evening activity, and his returns home, to the movement of the infection between Vidéotron and RISQ.

4. Analysis of Competing Hypotheses

In this section, we assess the evidence from this case and briefly examine two competing hypotheses that could explain our findings. First, we outline our reasoning for having high confidence that Omar Abdulaziz is the infected victim that we observed via DNS cache probing. Second, we entertain the hypothesis that some other individual is the Pegasus victim found in our data.

Hypothesis 1: Omar Abdulaziz's Phone was Infected

Based on the findings outlined in the report, we assessed that Omar Abdulaziz is the NSO victim identified during our DNS cache probing. This conclusion is based on several pieces of strong evidence.

Identification of a Pegasus Infection SMS on Abdulaziz's iPhone

We know that Abduldziz was targeted with NSO Pegasus because he was sent an SMS message containing a Pegasus exploit link (Figure 4). We found that the SMS had been viewed by Abdulaziz and that he believed that the message was related to his online order from Amazon, suggesting he may have clicked on the link. Based on prior research we know that clicking a Pegasus exploit link is sufficient for infecting a device with the spyware.

Matching a Known Pegasus Infection's Pattern of Life to Abdulaziz's Movements

Our DNS cache probing yielded a distinct pattern of life associated with the Quebec infection: on two occasions, it moved between Vidéotron, a consumer ISP, and RISQ, a university ISP, during the evenings and outside of the academic year. The pattern matched Abdulaziz's movements between his home, where he uses a Vidéotron connection, and the the university network (RISQ) where he performed his regular evening activity.

Abdulaziz is a Known Target of the Saudi Government

Abdulaziz has been a target of great interest to the Saudi government for several years. The government used a number of techniques in an attempt to discourage him from further advocacy, including revoking his scholarship in 2013 and apparently threatening his family and arresting his friends and brothers in 2018.

Hypothesis 2: Another Individual's Phone was Infected

It is possible that the Pegasus exploit link sent to Abdulaziz did not lead to his phone being infected. We are unable to prove that he clicked on the link and similarly lack forensic data from his iPhone that would prove an infection. However, were Abdulaziz's iPhone not infected, another victim would need to exist that meets the criteria in **Table 1**.

Evidence	Requirement
Pattern of life	During the period we were probing, the victim must have been located in Quebec, residing in a location serviced by Vidéotron. The victim must have been located approximately 20 minutes from a location serviced by the RISQ academic network where they connected during two evenings outside of the academic year, at the same times as Abdulaziz.
Of interest to Saudi Arabia	As Pegasus is expensive, and licensed by the number of concurrent infections, the victim must be of sufficient interest to the KINGDOM operator to warrant use of a Pegasus license.

Table 1: Quebec Victim Criteria

We are unaware of any individual besides Abdulaziz who fits both of these evidentiary criteria. In addition, no scheduling information provided by Abdulaziz fails to fit the pattern of life of the Pegasus infection.

Conclusion: Hypothesis 1 is the Most Plausible Explanation

Our prior work demonstrated that there is an infection with Pegasus in Quebec and that this infection phoned home on specific dates and times from specific networks. This finding, combined with the evidence that Abdulaziz was targeted with Pegasus and his obvious interest to the Saudi government, leads us to conclude with high confidence that the most plausible explanation for our findings is that Omar Abdulaziz is indeed the Pegasus victim that we identified using DNS cache probing.

5. Saudi Arabian Context: Human Rights in Turmoil

Saudi politics have been highly contentious since the death of King Abdullah in 2015. In an unusual move in June 2017, Saudi King Salman deposed his nephew Mohammed bin Nayef and appointed his son Mohammed bin Salman (known as "MbS") Crown Prince and heir apparent. Since taking power, MbS has engaged in an ambitious series of reforms accompanied by an aggressive crackdown against dissent, targeting both Saudi civil society and royalty alike.

Prior to becoming Crown Prince, MbS launched Saudi Vision 2030, an ambitious plan to diversify the country's economy away from oil, attract foreign investment, and improve the country's status as a regional economic and cultural power. He criticized the ultraconservative interpretation of Islam which has dominated the country and introduced a series of social reforms such as permitting the screening of movies and allowing women to drive.

Despite the more liberal nature of some of these reforms, they have been accompanied by an increase in repression, including a crackdown against women's rights defenders and other human rights activists. The crackdown against women's rights defenders was criticized by the United Nations High Commissioner for Human Rights and the European Parliament. Prior to this crackdown, the country was already one of the most repressive in the world, engaging in imprisonment of peaceful dissidents, widespread discrimination against women and religious minorities, and the extensive use of the death penalty for non-violent crimes.

In November 2017, MbS unexpectedly launched a purge, arresting hundreds of government ministers, princes, and prominent business people. While presented as an effort to root out corruption within the country's elite and to reclaim hundreds of billions of dollars in assets, the move was also widely seen as an effort by MbS to consolidate power. By removing existing princes from their ministries, he shook up the traditional balance of power amongst the ruling princes and is viewed by some as likely to become the most powerful Saudi monarch in decades.

The Canada-Saudi Human Rights Dispute

On August 2 and 3, 2018, two tweets sent by Canadian Minister of Foreign Affairs, Chrystia Freeland, and Global Affairs Canada's official government Twitter account

called on Saudi Arabia to free all "peaceful human rights activists," preceded a swift and aggressive response from Saudi Arabia. The two tweets were in response to Saudi Arabia's arrest of human rights activist Samar Badawi and her brother Raif. Samar Badawi had previously been arrested and subject to a travel ban in 2014 and Raif was imprisoned and sentenced to 1,000 lashes for setting up a website deemed critical of Islam. Raif Badawi's wife Ensaf Haidar has campaigned widely for her husband's release. She currently lives with their children in Quebec and was granted Canadian citizenship in July 2018.

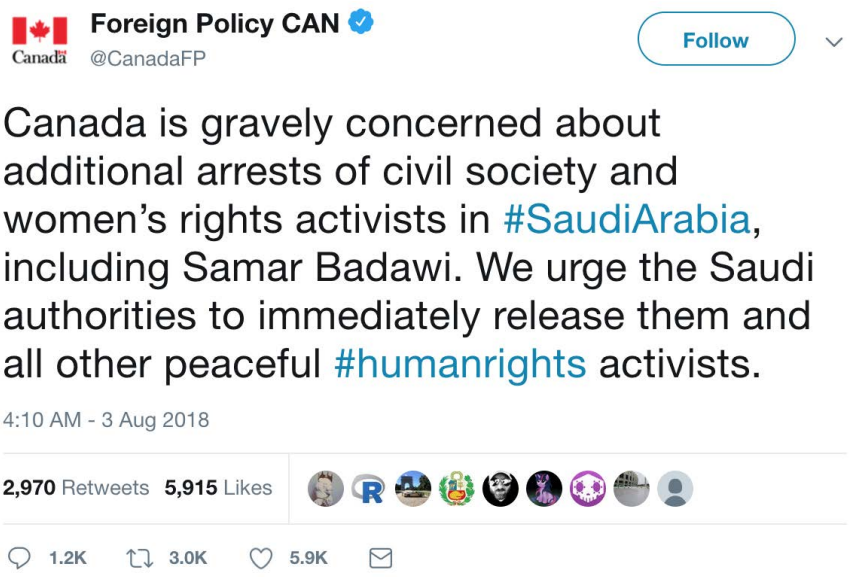

Figure 5: One of the tweets that reportedly precipitated the Saudi-Canada diplomatic row.

After these tweets, the Saudi Minister of Foreign Affairs responded with a series of tweets, calling the Canadian position "utterly false" and "interference in the internal affairs of the Kingdom of Saudi Arabia." The Minister also stated that that further action by Canada would mean that "we are allowed to interfere in Canada's internal affairs". The Saudi government expelled the Canadian ambassador from the country, recalled the Saudi ambassador to Canada, suspended flights between Saudi Arabia and Toronto, and implemented a freeze on "all new trade and investment transactions between Canada and Saudi Arabia". Student visas for Saudis studying in Canada were rescinded and all Saudi nationals receiving medical treatment in Canada were to be moved outside of the country. A "surge" of Saudi Twitter accounts began mobilizing against Canada, with some expressing support for Quebec's independence, and one tweet appearing to show an Air Canada plane flying into Toronto's CN Tower.

Figure 6: Image posted on Twitter by the verified "Infographic KSA" social media account, showing an Air Canada plane headed for Toronto's CN Tower. The account later apologized for posting the image, and was ordered shut down by the Saudi Ministry of Media.

The aggressive Saudi response was widely seen as an effort by MbS to exert a more forceful foreign policy, appeal to nationalist forces domestically, and reduce opposition to the reform process. Given the relatively modest economic relationship between Canada and Saudi Arabia, this conflict has also been interpreted as providing MbS with an opportunity to signal to western countries, at minimal cost to Saudi Arabia, that criticism of Saudi domestic affairs will not be tolerated.

Saudi Arabia's History of Commercial Spyware Abuse

Saudi Arabia has a history of using spyware purchased from foreign companies to target dissidents and critics. As of 2015, three agencies of the Saudi government were known customers of one commercial spyware company, Hacking Team. We suspect that at least one Saudi government agency is also a customer of another company, FinFisher.

In 2014, a Hacking Team customer, later revealed to be the Saudi Ministry of Interior's *General Investigation Directorate (GID)*, circulated links to an Android Application (APK) file containing a copy of the *Qatif Today* news application bundled with Hacking Team's RCS spyware. We were unable to identify specific targets of this

effort but we suspect that targets were in the *Qatif* region of Saudi Arabia, a Shia-dominated area which has been the site of protests against the Sunni-dominated Saudi government. Leaked Hacking Team emails reveal that the GID may have also used a booby-trapped Microsoft PowerPoint file called "Women Driving.pptx" to infect targets in 2015. The file (Figure 7) displayed a list of "The Top 10 Women Social Media Influencers" on the "Women Driving Campaign," and used a zero-day exploit for Adobe Flash to install Hacking Team's RCS spyware.

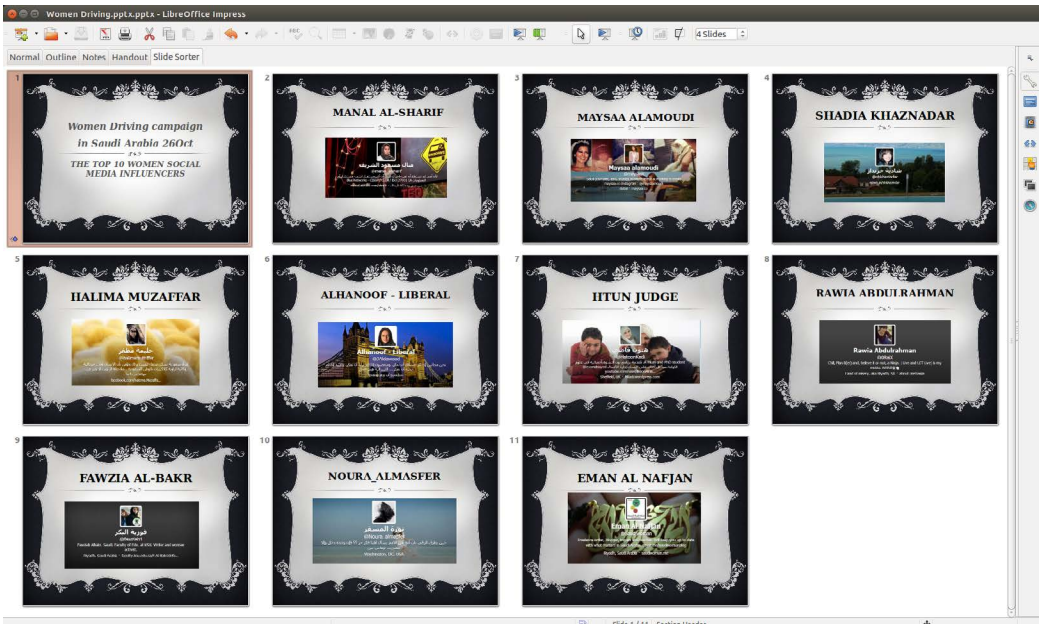

Figure 7: Bait file apparently used by the Saudi Ministry of Interior's General Investigation Directorate (GID) to infect targets with Hacking Team spyware in 2015.

The Hacking Team leaks revealed two further Saudi Arabian customers: the Saudi General Intelligence Presidency and the Saudi Ministry of Defense. In 2016, a company with links to the Saudi Arabian government purchased 20 percent of Hacking Team.

In June 2018, a staff member of human rights organization Amnesty International received a WhatsApp message about a protest in front of the Saudi Embassy in Washington, DC, in solidarity with political detainees in Saudi Arabia. The message contained a Pegasus exploit link. Additionally, UK-based Saudi dissident Yahya Assiri received an SMS message with a Pegasus exploit link; the message claimed that a court order had been issued against him.

6. Conclusion

We conclude with high confidence that a government customer of NSO Group targeted and infected Omar Abdulaziz, a Canadian permanent resident, with Pegasus spyware. The infection took place while he was on Canadian soil, after seeking and receiving asylum from the Canadian government. We further believe that this operator, which we named KINGDOM, is linked to the Saudi Arabia's government and security services.

The government customer identified by this investigation used a technology that NSO has marketed as a "cyber weapon" designed to catch terrorists and criminals, to target a young university student who peacefully and publicly voices his concerns about human rights via social media. It is unlikely that such an activity would have been conducted with the permission of Canadian authorities. If indeed it was conducted without Canadian authorization, the operators behind this targeting may have committed multiple Criminal Code offences, including willfully intercepting private communications contrary to section 184(1); unauthorized use of a computer contrary to section 342.1(1); and mischief in relation to computer data, contrary to section 430(1.1).

Six Years' Evidence of Commercial Spyware Abuse

This troubling case reinforces six years of findings by Citizen Lab showing that many governments and their intelligence services cannot resist abusing spyware that is purchased ostensibly for national security and criminal investigations.

In six years, we have observed *four* spyware companies (FinFisher, Hacking Team, Cyberbit, and NSO Group) make similar claims: their products are used for catching terrorists and criminals; they undertake due diligence before selling their products to a customer; and they investigate allegations of misuse, taking remedial actions if warranted. In each case, these companies' self-regulatory regimes proved inadequate: each company's products have been abused in ways that caused measurable harm to human rights defenders, journalists, lawyers working on behalf of victims of crimes, or civic media (e.g. bloggers).

As is typical of these sorts of cases, the use of spyware to target Omar Abdulaziz was one component of a broader campaign of repressive, punitive activities undertaken by a government in an effort to silence critics.

An Emerging Trend of *Serial Spyware Abusers*

There is another similarity worth noting: some countries emerge as serial spyware abusers. While NSO Group has repeatedly made public claims about due diligence conducted for each customer, they do not need to look far to find reports and allegations that link several current or recent customers with previously reported or alleged cases of spyware abuse using the products of companies like Hacking Team or Gamma Group (FinFisher spyware).

The full scope of Saudi Arabia's prior suspected use of government-exclusive spyware is unfortunately under-documented. However, public reports from numerous sources have indicated that Saudi security agencies have purchased and operated this technology for at least four years. Troublingly, previous reports, including research by Citizen Lab, point to political themes (such as documents supporting women driving) in some of those operations. Most recently, Amnesty International has reported that a staff member and a UK-based dissident blogger, were targeted by the same NSO operator described in this report.

Commercial Spyware and Global Cyber Insecurity

In many of the cases that Citizen Lab has investigated over the past six years, we have uncovered spyware customers targeting victims in other countries. These hostile acts of espionage likely violate laws in the countries where the victims are located. Cross-border targeting also carries both legal and diplomatic risk, and their repeated occurrence testifies to the still-evolving nature of jurisprudence surrounding cross-border, state-sponsored cyber attacks, especially when they target individuals, not other states.

Commercial Spyware: A Risky Investment

In the past several years it has become apparent that the commercial spyware world has attracted substantial interest among investors. For example, multiple investors have considered acquiring NSO Group, although in each case the deals appear to have fallen through. The findings of this research make it clear that NSO Group is not capable of preventing case after case of abuse of their product. These abuses have now led to multiple criminal investigations, and multiple lawsuits against NSO's customers and the company itself. An institutional investor, or a company considering an acquisition, is likely to recognize the legal and ethical risks associated with investing in such a company.

Appendix: IOCs for KINGDOM

In order to assist in tracking down additional abusive uses of Pegasus by the KINGDOM operator, we are releasing a set of domain names that appear to have been used by KINGDOM between October 2017 and August 2018.

Date	Target
Exploit domains (may appear in malicious SMS or WhatsApp messages)	akhbar-arabia[.]com
	all-sales[.]info
	arabnews365[.]com
	arabworld[.]biz
	daily-sport[.]news
	dinneraroundyou[.]com
	findmyplants[.]com
	housesfurniture[.]com
	kingdom-deals[.]com
	kingdom-news[.]com
	mideast-today[.]com
	muslim-world[.]info
	news-gazette[.]info
	nouvelles247[.]com
	promosdereve[.]com
	social-life[.]info
	sunday-deals[.]com
	wonderfulinsights[.]com
Command and Control (C&C) domain names (may appear in the Internet traffic of infected devices or DNS logs)	beststores4u[.]com
	cheapapartmentsaroundme[.]com

Table 2: Domain names employed by the KINGDOM operator