Short Background: Citizen Lab Research on FinFisher Presence in Malaysia

1. What is the Citizen Lab?

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto. We have have been conducting research and development; policy engagement; and capacity building activities since 2001.

We are independent of government or corporate interests, and publish on the basis of evidence-based, peer reviewed research. Our focus is on cyberspace security and governance issues from the perspective of civil society, with a special focus on "lifting the lid" on practices that undermine human rights online, including censorship, surveillance, and warfare.

Financial support for the Citizen Lab's research and development has come from the Ford Foundation, the Open Society Institute, the Social Sciences and Humanities Research Council of Canada, the International Development Research Centre, The Canada Centre for Global Security Studies, the John D. and Catherine T. MacArthur Foundation, the Donner Canadian Foundation, and the Walter and Duncan Gordon Foundation.

2. What is FinFisher?

FinFisher[1] is made by a company called Gamma International and it is marketed as a powerful tool for accessing the computers of suspected criminals and terrorists secretly. The FinFisher Suite is described by its distributors, Gamma International UK Ltd., as "Governmental IT Intrusion and Remote Monitoring Solutions."[2] Promotional materials that have been leaked describe the tools as providing a wide range of intrusion and monitoring capabilities.[3]

Once it has infected your computer, FinFisher is not detected by anti-virus or anti-spyware software. Some of FinFisher's capabilities are the following: **steals passwords from your computer, allowing access to your e-mail accounts**; **wiretaps your Skype calls; turn on your computer's camera and microphone to record conversations and video from the room that you are in.**

---

[1] When we refer to "FinFisher" or "FinSpy" in this report, we are referring to software that is consistent with indicia of Gamma International's FinFisher and FinSpy products. Gamma International has refused to confirm or deny whether it sold specific software to any particular customer, and we have no information about what, if any, commercial arrangements were involved.

[1]

[2] http://www.finfisher.com/FinFisher/en/index.php

[3] http://owni.eu/2011/12/15/finfisher-for-all-your-intrusive-surveillance-needs/#SpyFiles

Gamma International markets FinFisher as a tool used by government law enforcement and intelligence agencies to monitor suspected criminals, but our research findings suggested that it is being used more broadly.

3. What are the Citizen Lab's recent research findings on FinFisher?

In 2012, the Citizen Lab analyzed emails sent to pro-democracy Bahraini activists, which were passed to us by a Bloomberg reporter, and found evidence that they contained malicious software (malware) called FinSpy, part of the FinFisher spyware tool kit. The term "FinSpy" itself appeared in the malware's code.

In a report titled "From Bahrain with Love: FinFisher's Spy Kit Exposed?", we identified and classified the malware to better understand the attacks and the risk to victims. In order to accomplish this, we undertook several different approaches during the investigation. We infected a virtual machine (VM) with the malware, as well as directly examining the samples through static and dynamic analysis. We monitored the filesystem, network, and running operating system of the infected VM.

Since then, the Citizen Lab has published a number of reports on FinFisher, such as "The SmartPhone Who Loved Me: FinFisher Goes Mobile?", "Backdoors are Forever: Hacking Team and the Targeting of Dissent?", and "You Only Click Twice: FinFisher's Global Proliferation."

Our research suggested that FinFisher is being used for surveillance beyond suspected criminal activity and that there has been a global proliferation in the use of FinSpy. We identified 36 active FinSpy command & control servers, including 30 previously-unknown servers. Our list of servers is likely incomplete, as some FinSpy servers employ countermeasures to prevent detection. Including servers discovered last year, we now count FinSpy servers in 25 countries, including countries with troubling human rights records.[4] It is important to note that the presence of a FinFisher Command & Control server in a country does not necessarily imply that the country's law enforcement, security, or intelligence services are running the server.

4. What are the main findings of FinFisher in Malaysia?

In March 2013, we searched the Internet, looking for computers (servers) that gathered stolen information (passwords, Skype calls, audio/video recordings) from computers infected with FinFisher. We found one of these FinFisher servers in Malaysia. However, the presence of a FinFisher server in Malaysia does not necessarily mean that the Malaysian government, law enforcement, security, or intelligence services are running the server.

[4] https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

After The New York Times reported on the presence of FinFisher server in Malaysia[5], a news website called "The Malaysian Insider" (TMI) published an article with the headline stating "Malaysia Uses Spyware against Own Citizens, NYT Reports". In response, the Malaysian Communications and Multimedia Commission accused TMI of false reporting.[6] Regardless, the Malaysian government did not confirm or deny if they were using FinFisher.

We have now identified a Malaysian election-related document that also contains a piece of surveillance software that will spy on you.

Our findings so far **do not make it possible to say who has put FinFisher in this document, or who is circulating it.** But because FinFisher is explicitly only sold to governments we think that it is reasonable to assume that some government actor is responsible.

We do not know how many people were infected and we do not know exactly who was the target of this document. But while we cannot make definitive statements about the actors behind the booby-trapped candidate list, the contents of the document suggest that the campaign targets Malay speakers who are interested or involved in Malaysia's 2013 General Elections.

[5] http://bits.blogs.nytimes.com/2013/03/13/researchers-find-25-countries-using-surveillance-software/
[6] http://www.digitalnewsasia.com/digital-economy/mcmc-probes-the-malaysian-insider-over-spyware-story