Latar Belakang Singkat: Penelitian Citizen Lab Mengenai Kehadiran FinFisher di Indonesia

1. Mengenai Citizen Lab

Citizen Lab merupakan laboratorium penelitian interdisipliner yang berbasis di Munk School of Global Affairs, University of Toronto. Kami telah melakukan penelitian, keterlibatan kebijakan (*policy engagement*) dan pengembangan kapasitas (*capacity building*) sejak tahun 2001.

Penelitian kami independen dari kepentingan pemerintah atau swasta. Kami mempublikasikan hasil penelitian berdasarkan bukti yang telah melalui proses penelaahan sejawat (*peer review*).

Fokus penelitian kami adalah pada masalah keamanan dan tata kelola Internet dari perspektif masyarakat sipil, khususnya untuk "mengangkat tutup" dari praktek-praktek yang tidak menghormati perlindungan hak asasi manusia secara *online*, termasuk pensensoran, pengintaian, dan peperangan.

Dukungan dana untuk penelitian kami telah datang dari Ford Foundation, Open Society Institute, Social Sciences and Humanities Research Council of Canada, International Development Research Centre, Canada Centre for Global Security Studies, John D. and Catherine T. MacArthur Foundation, Donner Canadian Foundation, dan Walter and Duncan Gordon Foundation.

2. Mengenai FinFisher

FinFisher[1] dibuat oleh perusahaan dengan nama Gamma International dan dipasarkan sebagai alat yang sangat canggih yang dapat mengakses komputer para tersangka kriminal dan terorisme secara diam-diam. Program FinFisher digambarkan oleh sang distributor, Gamma International UK Ltd., sebagai alat agar pemerintah dapat melakukan penggangguan dan pengintaian jarak jauh ("*Governmental IT Intrusion and Remote Monitoring Solutions*").[2] Materi promosi yang telah dibocorkan ke masyarakat umum menjelaskan bahwa alat tersebut memiliki

[1] Ketika kita menyebut "FinFisher" atau "FinSpy" dalam laporan ini, kita mengacu kepada perangkat lunak yang konsisten dengan karakter dari produk FinFisher dan FinSpy buatan Gamma International. Gamma International telah menolak untuk mengkonfirmasi atau menyangkal apakah mereka menjual perangkat lunak khusus untuk setiap pelanggan tertentu, dan kita tidak memiliki informasi tentang apa, jika ada, perjanjian komersial terlibat.

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

berbagai macam kemampuan pengganggguan dan pengintaian.[3]

Setelah FinFisher menginfeksi komputer Anda, maka FinFisher tidak dapat terdeteksi oleh perangkat *anti-virus* atau *anti-spyware*. Beberapa kemampuan FinFisher adalah sebagai berikut: **mencuri berbagai kata kunci dari komputer Anda, memungkinkan akses ke akun email Anda, menyadap perbincangan Anda di Skype, menyalakan kamera dan mikrofon di komputer untuk merekam percakapan dan video Anda. FinFisher juga dapat menginfeksi telepon genggam sekaligus komputer Anda.**

Gamma International memasarkan FinFisher sebagai alat untuk digunakan oleh aparat penegak hukum dan badan intelijen untuk memantau tersangka kriminal, tetapi penelitian kami menunjukkan bahwa alat tersebut digunakan secara lebih luas.

3. Penelitian Citizen Lab mengenai FinFisher

Pada tahun 2012, Citizen Lab menganalisa email yang dikirimkan ke para aktivis pro-demokrasi di Bahrain, yang diberikan ke kami oleh seorang reporter dari majalah Bloomberg, dan menemukan bahwa email tersebut mengandung *malware* yang disebut FinSpy, yang merupakan bagian dari perangkat *spyware* FinFisher. Istilah “FinSpy” itu sendiri ditemukan di dalam kode sumber *malware* tersebut.

Dalam laporan dengan judul “From Bahrain with Love: FinFisher’s Spy Kit Exposed?”, kami mengidentifikasi dan mengklasifikasi *malware* tersebut agar dapat lebih memahami serangan dan risiko kepada korban. Untuk mencapai hal ini, kami menggunakan beberapa cara yang berbeda dalam penyelidikan. Kami menginfeksi mesin virtual (*virtual machine* (VM)) dengan *malware*, serta langsung memeriksa sampel melalui analisis statis dan dinamis. Kami memantau *filesystem*, jaringan, dan menjalankan *operating system* dari VM yang terinfeksi.

Sejak itu, Citizen Lab telah menerbitkan sejumlah laporan tentang FinFisher, seperti “The SmartPhone Who Loved Me: FinFisher Goes Mobile?”, “Backdoors are Forever: Hacking Team and the Targeting of Dissent?”, “You Only Click Twice: FinFisher’s Global Proliferation” dan For Their Eyes Only: The Commercialization of Digital Spying

Penelitian kami menunjukkan bahwa FinFisher digunakan lebih dari sekedar untuk pengawasan dari mereka yang diduga sebagai pelaku kriminal dan bahwa telah terjadi proliferasi secara global dalam penggunaan FinSpy. Kami mengidentifikasi 36 *command-and-control servers* FinSpy yang aktif, termasuk 30 *server* yang sebelumnya tidak kami ketahui. Daftar tersebut kemungkinan tidak lengkap, karena beberapa *server* FinSpy menggunakan alat-alat atau cara-cara tertentu untuk mencegah deteksi. Termasuk sejumlah *server* yang telah kita temukan tahun lalu, kita menghitung adanya *server* FinSpy di 25 negara, termasuk negara-negara dengan

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

sejarah perlindungan hak asasi manusia yang buruk.[4]

Penting untuk dicatat bahwa kehadiran dari *command-and-control server* FinFisher dalam satu negara belum tentu berarti bahwa *server* tersebut dijalankan oleh para aparat penegak hukum, keamanan, atau badan intelijen negara tersebut.

4. Penemuan FinFisher in Indonesia

Kami menelusuri Internet, mencari komputer (*server*) yang mengumpulkan informasi yang telah di curi (password, percakapan Skype, rekaman audio / video) dari komputer yang terinfeksi dengan FinFisher. Kami menemukan delapan *server* FinFisher di Indonesia, pada tiga penyedia jasa Internet (*Internet service provider* (ISP)) yang berbeda yaitu PT Telkom, PT Matrixnet Global dan Biznet (lihat Tabel 1).

Menanggapi penemuan kami, juru bicara Kementerian Komunikasi dan Informatika (Kominfo) berjanji bahwa pemerintah akan mengambil "tindakan tegas" terhadap ISP jika mereka ditemukan telah melakukan pengintaian, dan menyebutkan bahwa mereka bisa terancam hukuman hingga lima belas tahun penjara. Namun, karena Gamma International menyatakan bahwa mereka hanya menjual produk FinFisher kepada pemerintah, maka akan mengejutkan apabila ternyata *server* FinFisher tersebut digunakan oleh para ISP.

Kehadiran *server* FinFisher di Indonesia belum tentu berarti bahwa pemerintah, penegak hukum, keamanan, atau badan intelijen Indonesia menjalankan server tersebut.

Tabel 1: Daftar *server* FinFisher di Indonesia

IP Address	**Operator**
118.97.xxx.xxx	PT Telkom
118.97.xxx.xxx	PT Telkom
118.97.xxx.xxx	PT Telkom
103.28.xxx.xxx	PT Matrixnet Global
103.28.xxx.xxx	PT Matrixnet Global
112.78.143.34	Biznet ISP
112.78.143.26	Biznet ISP
112.78.xxx.xxx	Biznet ISP

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

FinFisher yang berada dalam komputer dapat digunakan untuk mencuri data dan mengirimkannya kembali kepada yang mengintai Anda melalui Internet.

FinFisher untuk telepon genggam juga dapat mengirimkan data yang telah dicuri melalui SMS. Kami menemukan satu sampel dari FinFisher versi ponsel dengan nomor telepon asal Indonesia (+62), yang digunakan oleh *spyware* tersebut untuk mengirim data yang dicuri melalui SMS. Kita tidak tahu siapa yang menjadi target sampel ini, tapi kami pikir orang-orang yang menjadi sasaran kemungkinan besar berada di Indonesia, karena nomor tersebut merupakan nomor telepon Indonesia.

Nomor telepon yang kami identifikasi dalam sampel FinFisher adalah:

+6281310xxxxx4 – Indonesia