Emergency VPN

Analyzing Mobile Network Traffic to Detect Digital Threats

Veronica Valeros, veronica.valeros@aic.fel.cvut.cz, @verovaleros
Sebastian Garcia, sebastian.garcia@agents.fel.cvut.cz, @eldracote
Civilsphere Project, Stratosphere Laboratory, Czech Technical University in Prague
www.civilsphereproject.org

Source: New York Times

Maati Monjib

Historian

Source: Citizen Lab

Alberto Nisman

Lawyer

Source: Human Rights Watch

Ahmed Mansoor

Activist

Source: Citizen Lab

Simón Barquera

Researcher

Source: Citizen Lab

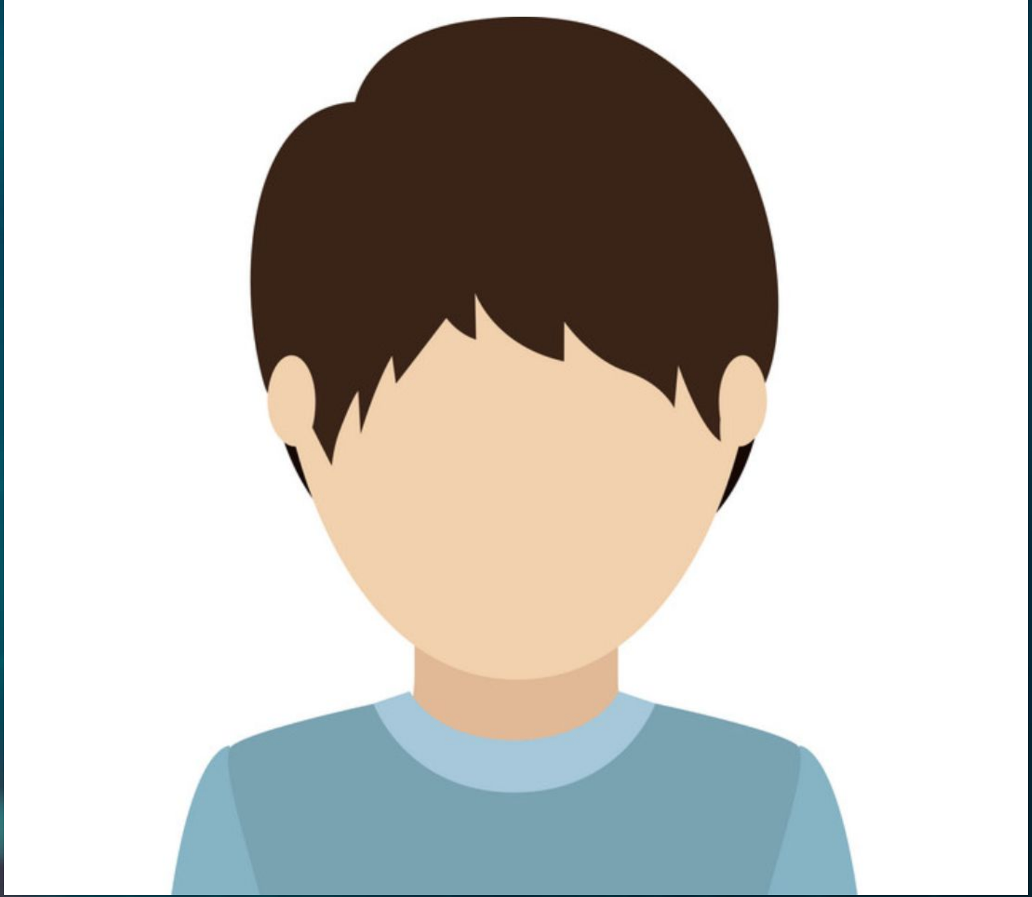
Karla Salas

Lawyer

Source: Al Jazeera

Griselda Triana

Widow



Source: Citizen Lab

Emilio Aristegui

Lawyer son (minor)

Governments use spyware to surveil, abuse, imprison and kill individuals

WHAT CAN WE DO IF WE SUSPECT OUR PHONE IS COMPROMISED?

Careful analysis of a mobile device to identify the cause of an infection. Costly. Takes time.

FORENSIC ANALYSIS

Restoring the phone to its original state.
Does not help for certain infections.

FACTORY RESET

Simple solution.
Very costly for the users.

CHANGE PHONES

Analysis of the network traffic to identify suspicious connections

TRAFFIC ANALYSIS

How can we know if our phone is compromised?

Our Proposal. Emergency VPN

What is the EVPN?

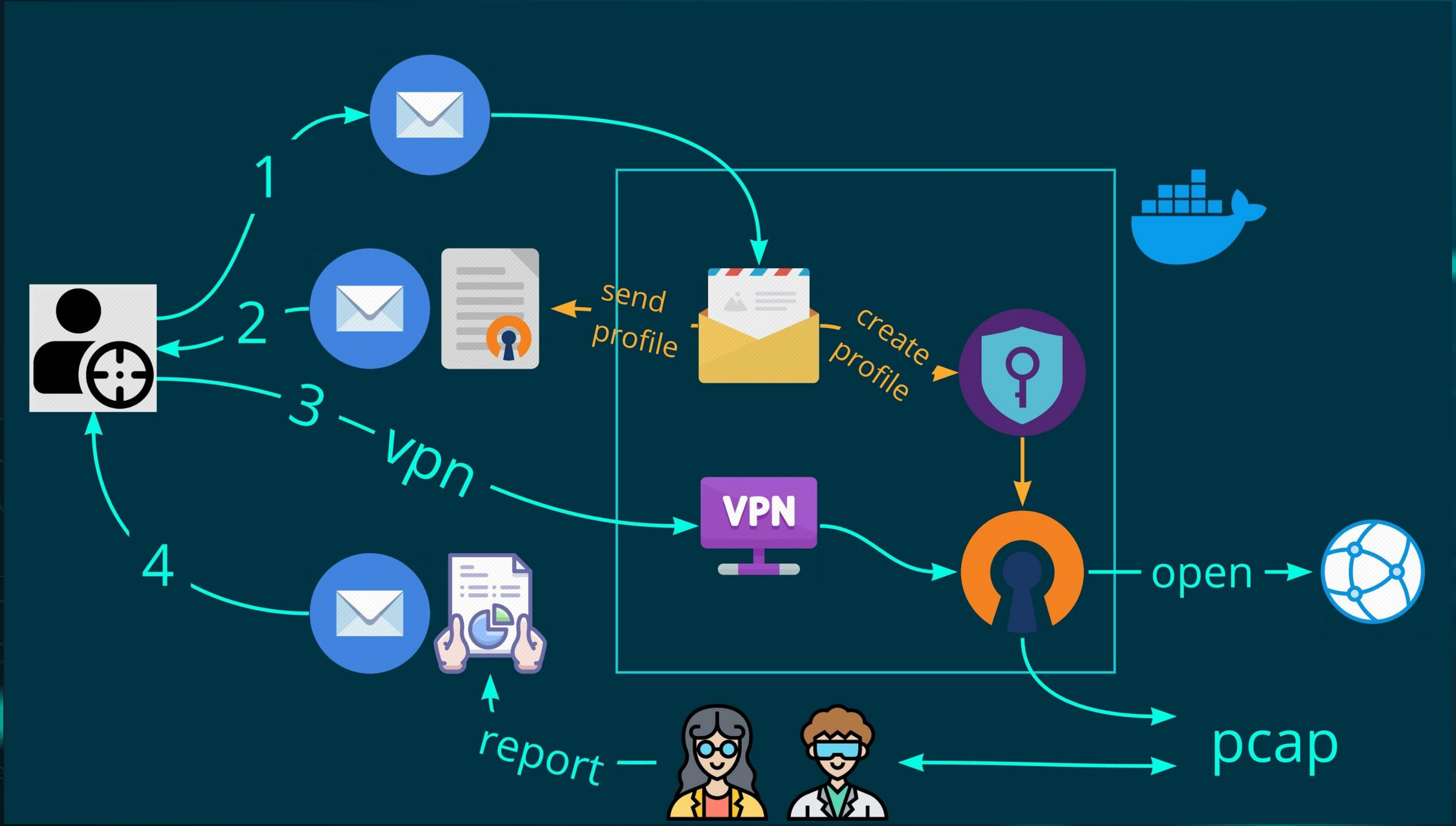
Free OpenVPN service for your phone, going through our University

Security Analysis Service of the Traffic of your Phone. 3 days max

Analysis by experts and tools

Free Software

How does the EVPN work?



Advantages of EVPN

Immediate Analysis

Technology + Expertise

As anonymous as we can do it

Continuous Research

Report back to you

Free to use any time you feel at risk

Insights from EVPN operations

Active since mid 2018

Analyzed 111 cases

60% Android devices

82 GB of traffic analyzed

3,200 hours of traffic analyzed

95% of issues are caused by normal apps

The most common issues of mobile users

GEOLOCATION LEAKED

Plain text. You don’t need to be infected to be found.

INSECURE APPS

Applications use insecure protocols that endanger the user by leaking their data

PERSONAL DATA

Email, phone number, user behavior, preferences

IMEI & IMSI

Unique information that can help track and locate a user.

Important Cases

Trojans

Not targeted trojans designed to steal money from their victims

P2P with malicious files

Peer to peer applications advertised as file sharing but used to spread malware

Why not more?

We need to reach the right audience, at the right time

Do you believe you are at risk?

Do you know somebody at risk?

Contact us

civilsphere@aic.fel.cvut.cz
+420 778 577 766

THANKS!

civilsphere@aic.fel.cvut.cz
+420 778 577 766
www.civilsphereproject.org

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**.