Lessons learned from Securing Civil Society

BSides Zurich

14 September 2019

Who am I

- Italian, based in Berlin.
- Head of Security Lab at **Amnesty International**, since 2016.
- Advisor, formerly a Senior Research Fellow at **Citizen Lab**.
- Started working in information security ~10 years ago.
- Been researching digital threats to civil society for the last ~7 years.
- Founder *Security Without Borders*, *Cuckoo Sandbox*, *Viper Framework* and *Malwr.com*.

Amnesty Tech work on Digital Security

- We work with external Human Rights Defenders (HRDs).
- We have technologists distributed across our regional offices.
  - Berlin, Dakar, Nairobi, Tunis, Beirut.
- We do threat research, digital security advisory and mentorship, we build tools and services, we respond to incidents, etc.

The problem

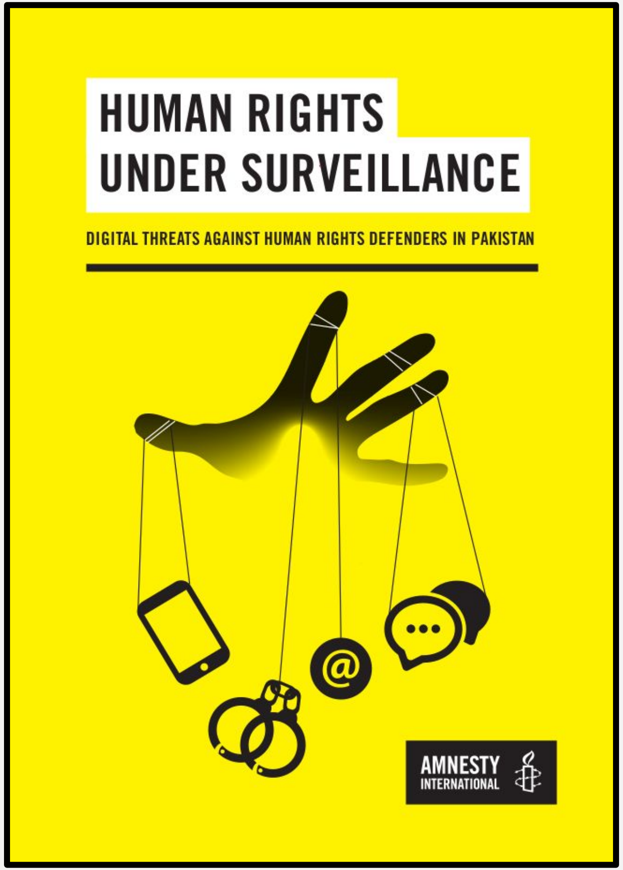
Technology has become an integral part of modern society, including civil society. **Human Rights Defenders make use of Internet and social media platforms to amplify much of their work today**.

At the same time, technology has also become a powerful tool for repression. HRDs are increasingly targets of **digital surveillance** and other **online threats**, for the purpose of **infiltration**, **monitoring** and **intimidation**.

Agenda

- The **threats**
- The **challenges**
- The **opportunities**

Threats

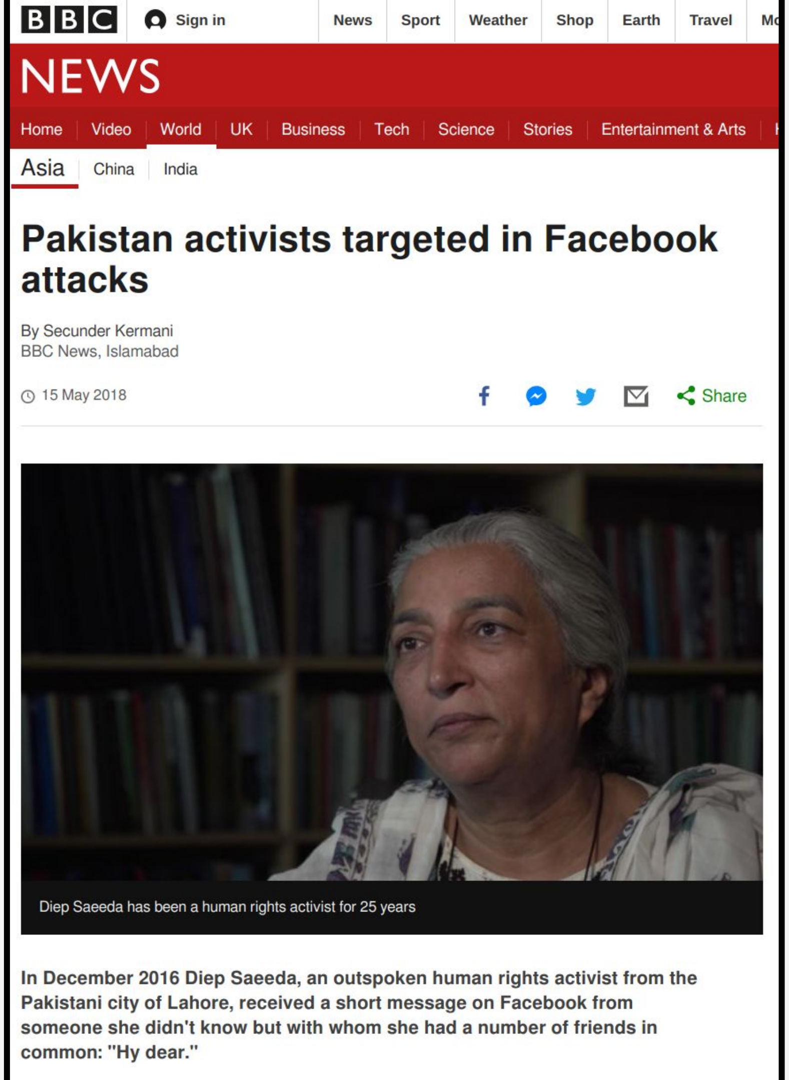


HUMAN RIGHTS UNDER SURVEILLANCE

DIGITAL THREATS AGAINST HUMAN RIGHTS DEFENDERS IN PAKISTAN

AMNESTY INTERNATIONAL

https://www.amnesty.org/en/documents/asa33/8366/2018/en/



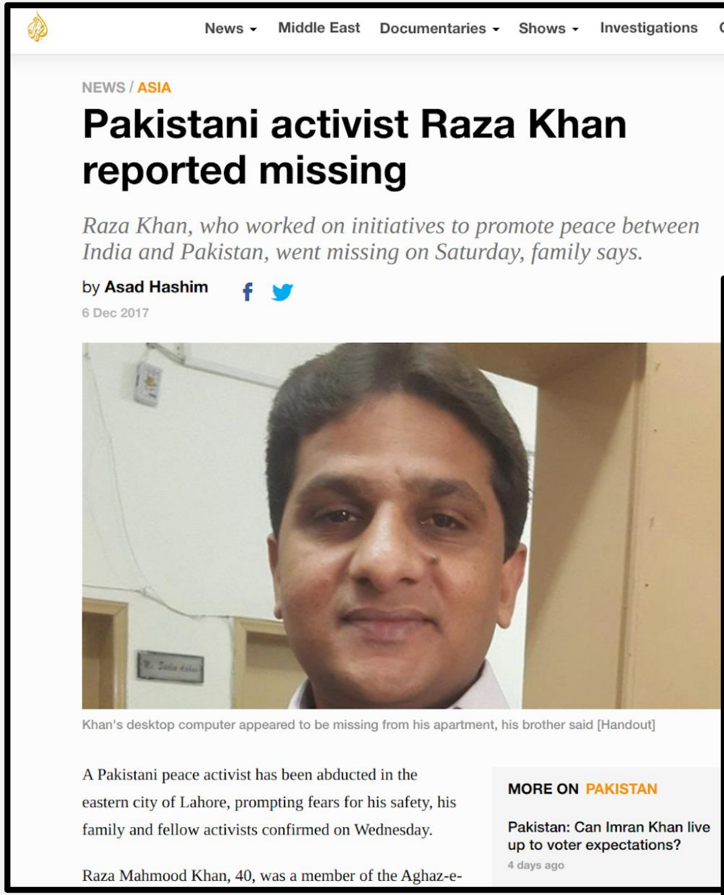
Pakistan activists targeted in Facebook attacks

By Secunder Kermani
BBC News, Islamabad

15 May 2018

Diep Saeeda has been a human rights activist for 25 years

In December 2016 Diep Saeeda, an outspoken human rights activist from the Pakistani city of Lahore, received a short message on Facebook from someone she didn't know but with whom she had a number of friends in common: "Hy dear."



NEWS / ASIA

Pakistani activist Raza Khan reported missing

Raza Khan, who worked on initiatives to promote peace between India and Pakistan, went missing on Saturday, family says.

by **Asad Hashim**

6 Dec 2017

Khan's desktop computer appeared to be missing from his apartment, his brother said [Handout]

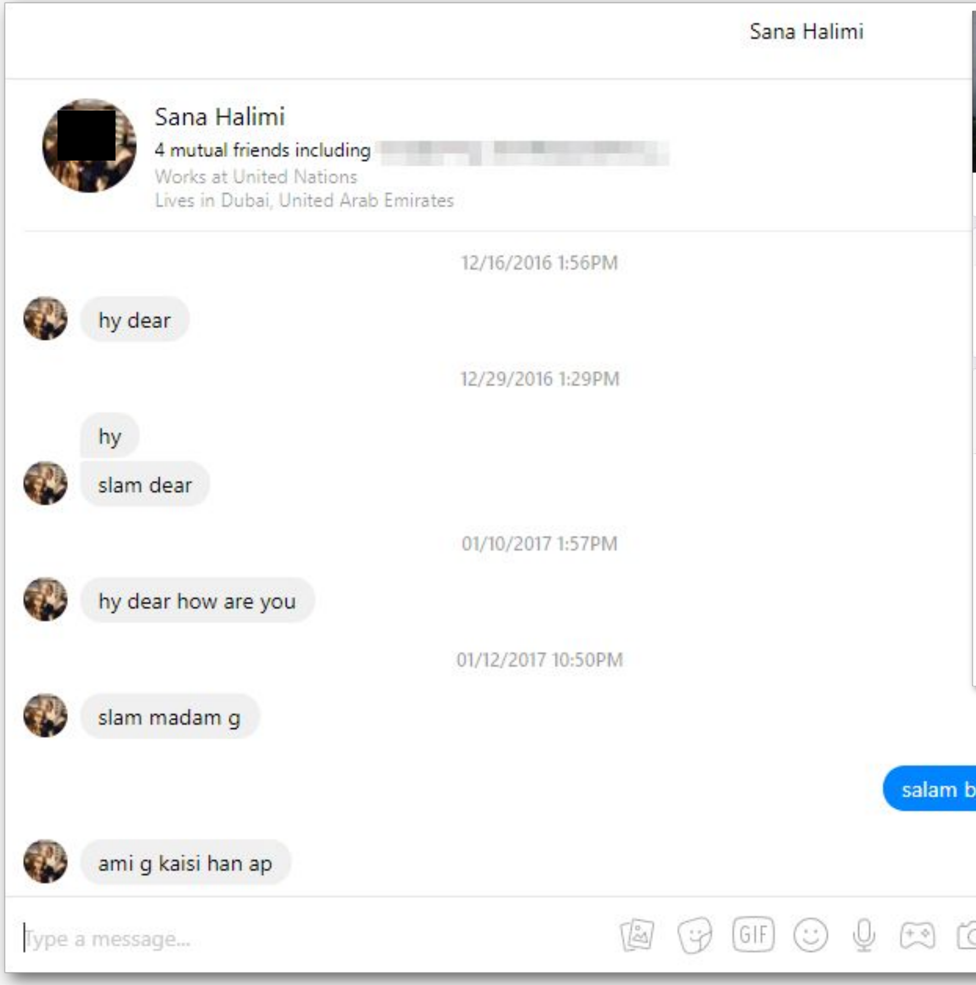
A Pakistani peace activist has been abducted in the eastern city of Lahore, prompting fears for his safety, his family and fellow activists confirmed on Wednesday.

Raza Mahmood Khan, 40, was a member of the Aghaz-e-

MORE ON PAKISTAN

Pakistan: Can Imran Khan live up to voter expectations?

4 days ago



Sana Halimi

Sana Halimi
4 mutual friends including [redacted]
Works at United Nations
Lives in Dubai, United Arab Emirates

12/16/2016 1:56PM

hy dear

12/29/2016 1:29PM

hy

slam dear

01/10/2017 1:57PM

hy dear how are you

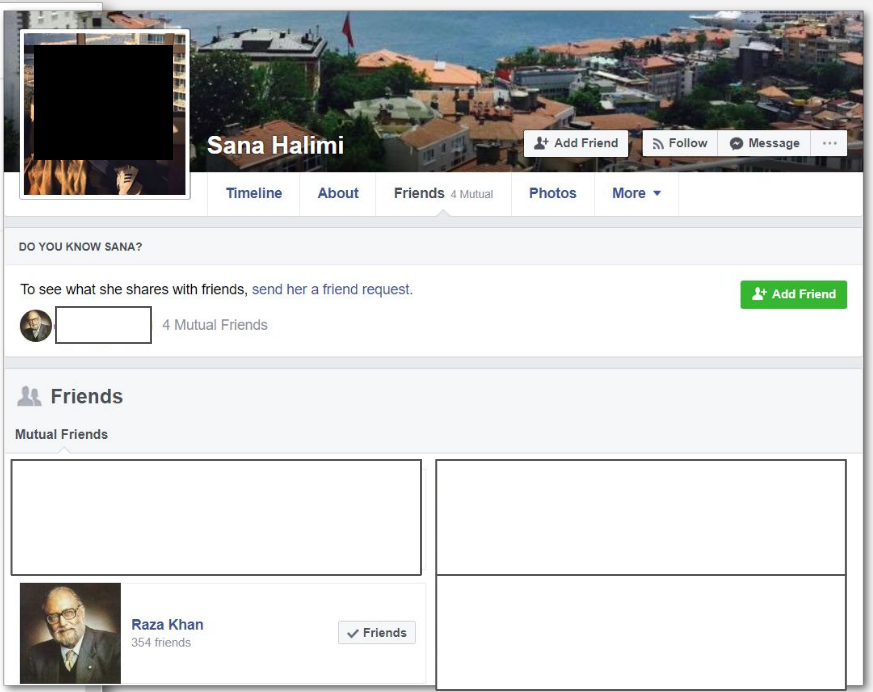
01/12/2017 10:50PM

slam madam g

salam be

ami g kaisi han ap

Type a message...



Sana Halimi

DO YOU KNOW SANA?

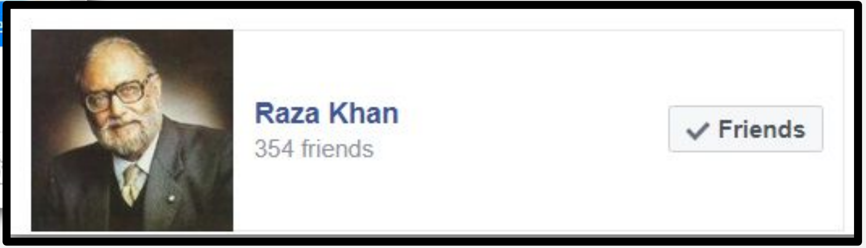
To see what she shares with friends, send her a friend request.

4 Mutual Friends

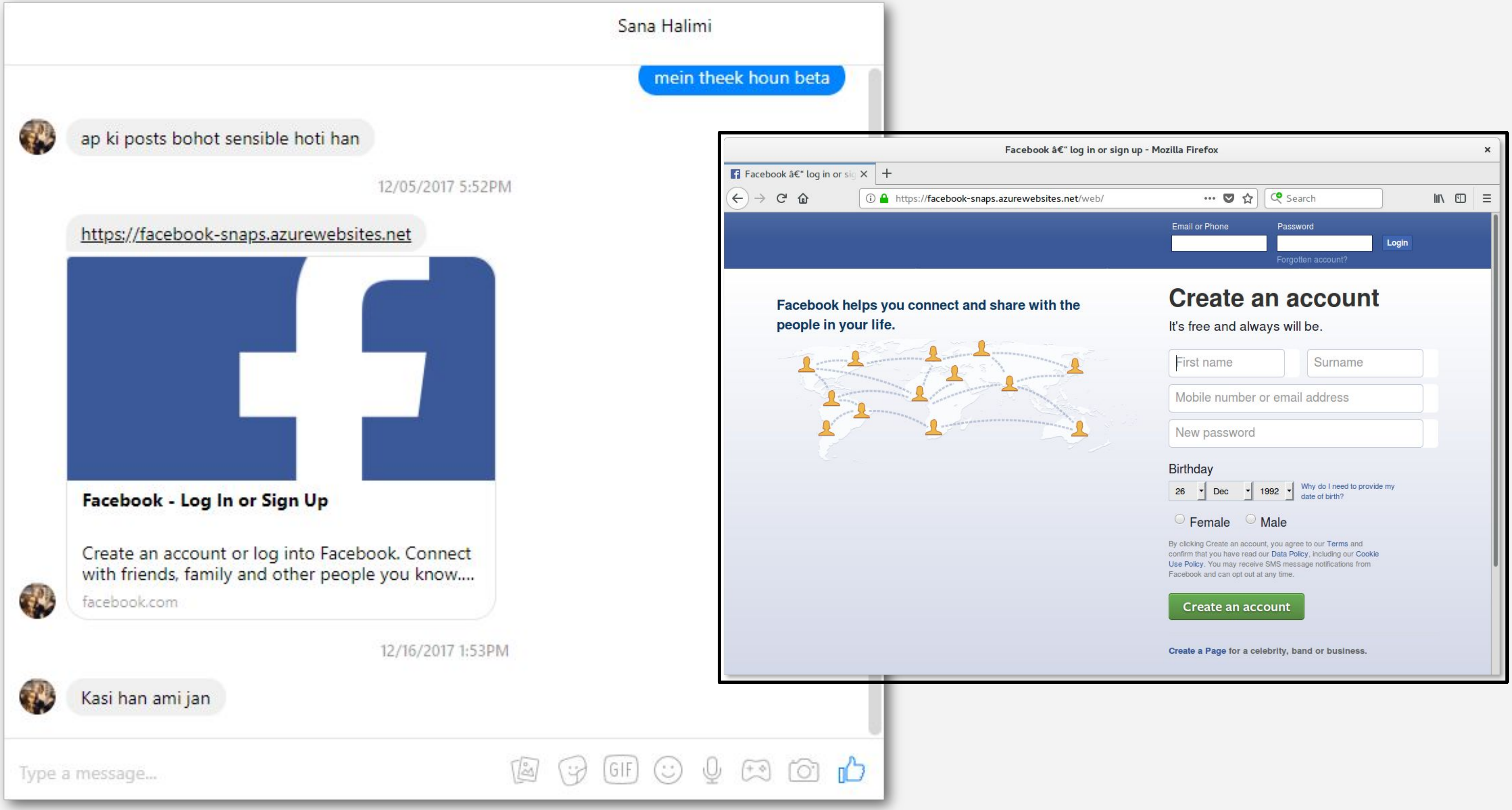
Friends

Mutual Friends

Raza Khan
354 friends



Raza Khan
354 friends



Sana Halimi

mein theek houn beta

ap ki posts bohot sensible hoti han

12/05/2017 5:52PM

https://facebook-snaps.azurewebsites.net

Facebook - Log In or Sign Up

Create an account or log into Facebook. Connect with friends, family and other people you know....

facebook.com

12/16/2017 1:53PM

Kasi han ami jan

Facebook â€" log in or sign up - Mozilla Firefox

Facebook â€" log in or sig

https://facebook-snaps.azurewebsites.net/web/

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

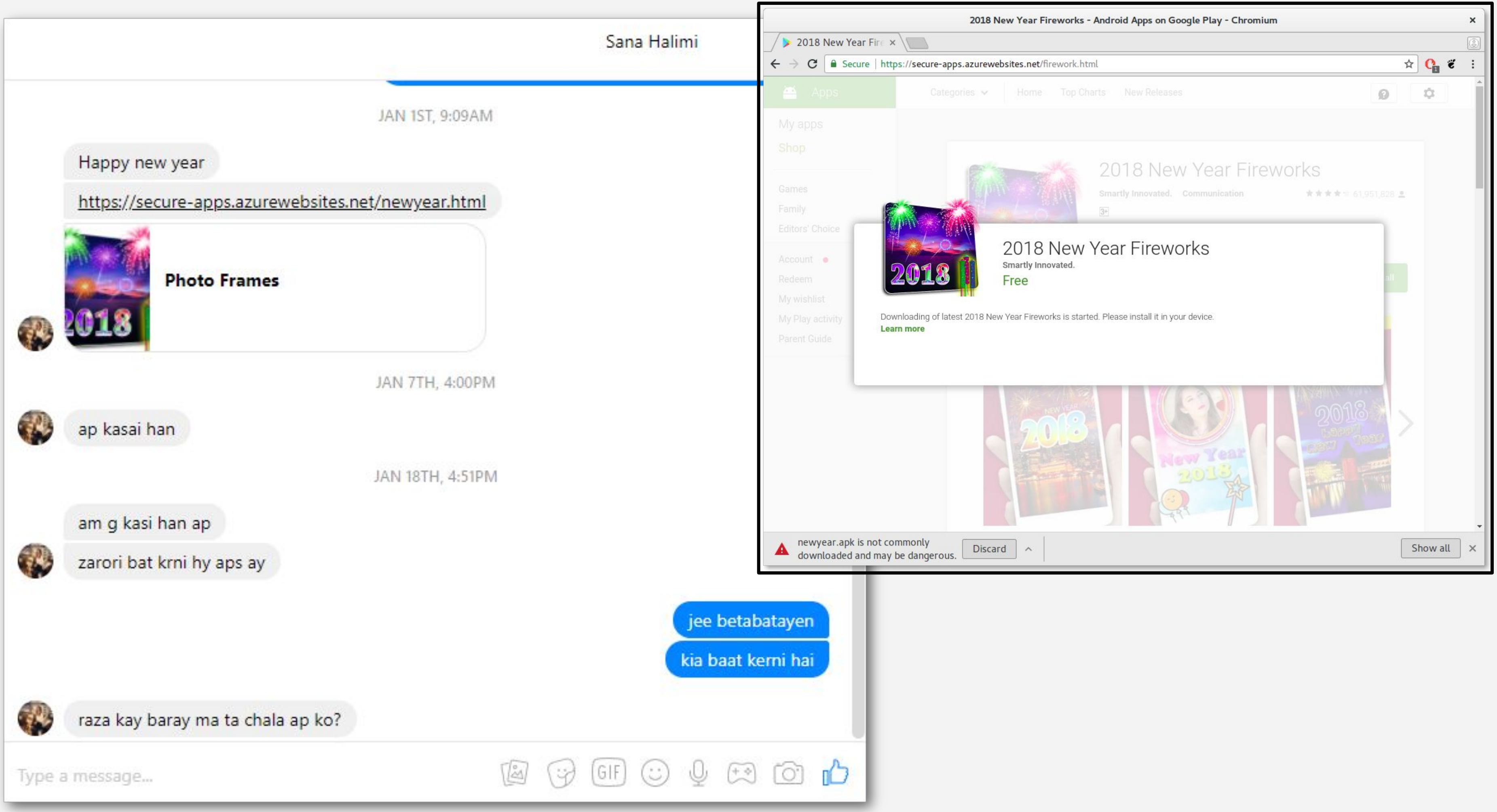
Birthday

26 Dec 1992

○ Female ○ Male

By clicking Create an account, you agree to our Terms and confirm that you have read our Data Policy, including our Cookie Use Policy. You may receive SMS message notifications from Facebook and can opt out at any time.

Create a Page for a celebrity, band or business.



Sana Halimi

JAN 1ST, 9:09AM

Happy new year

https://secure-apps.azurewebsites.net/newyear.html

Photo Frames

JAN 7TH, 4:00PM

ap kasai han

JAN 18TH, 4:51PM

am g kasi han ap

zarori bat krni hy aps ay

jee betabatayen

kia baat kerni hai

raza kay baray ma ta chala ap ko?

Type a message...

2018 New Year Fireworks - Android Apps on Google Play - Chromium

2018 New Year Fir

Secure | https://secure-apps.azurewebsites.net/firework.html

Apps

Categories Home Top Charts New Releases

My apps

Shop

Games

Family

Editors' Choice

Account

Redeem

My wishlist

My Play activity

Parent Guide

2018 New Year Fireworks

Smartly Innovated. Communication

3+

2018 New Year Fireworks

Smartly Innovated.

Free

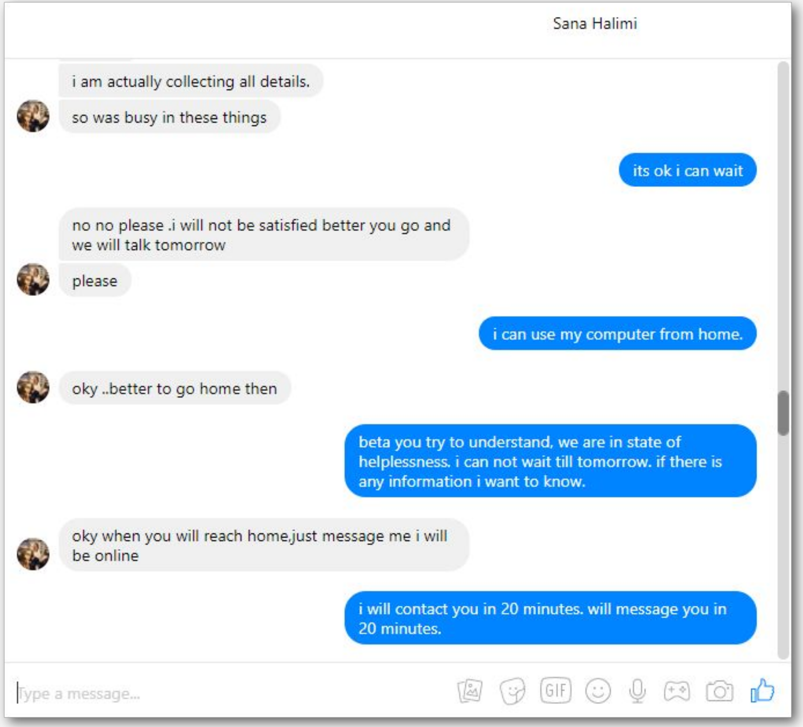
Downloading of latest 2018 New Year Fireworks is started. Please install it in your device.

Learn more

newyear.apk is not commonly downloaded and may be dangerous.

Discard

Show all



Sana Halimi

i am actually collecting all details.

so was busy in these things

its ok i can wait

no no please .i will not be satisfied better you go and we will talk tomorrow

please

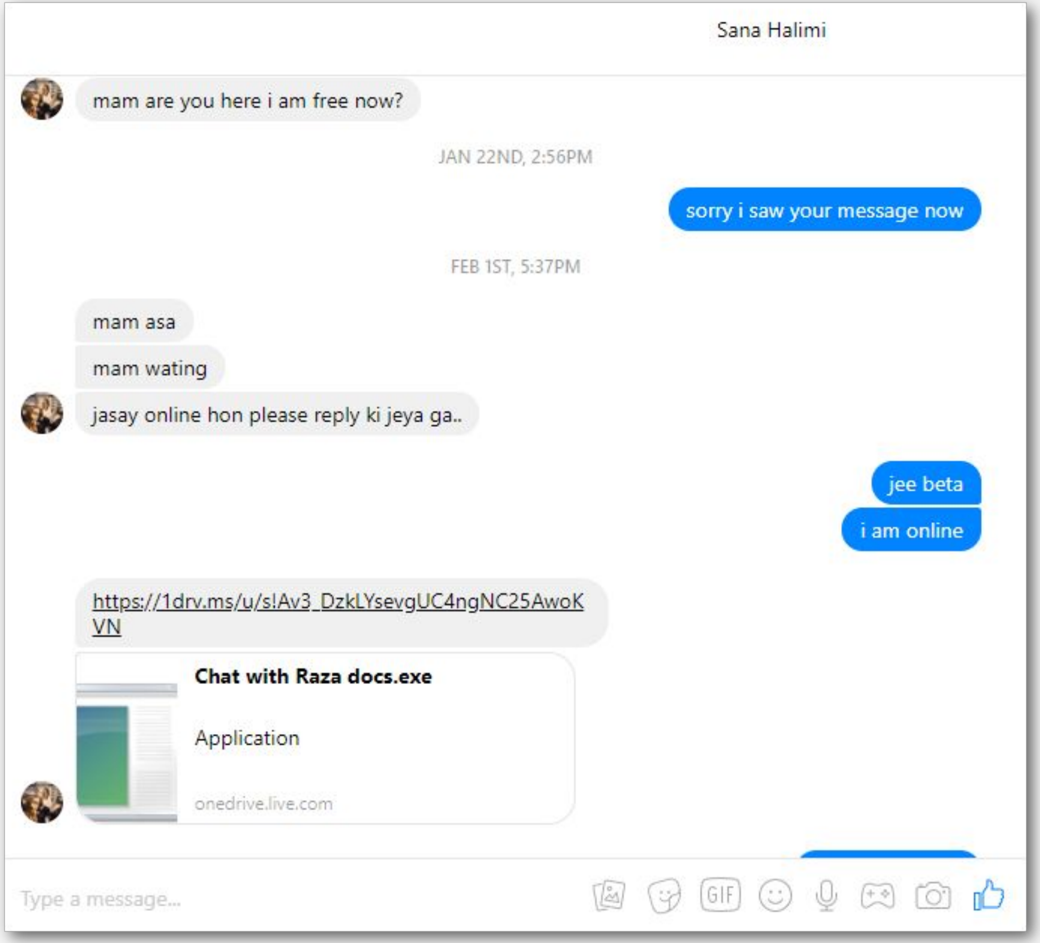
i can use my computer from home.

oky ..better to go home then

beta you try to understand, we are in state of helplessness. i can not wait till tomorrow. if there is any information i want to know.

oky when you will reach home,just message me i will be online

i will contact you in 20 minutes. will message you in 20 minutes.



Sana Halimi

mam are you here i am free now?

JAN 22ND, 2:56PM

sorry i saw your message now

FEB 1ST, 5:37PM

mam asa

mam wating

jasay online hon please reply ki jeya ga..

jee beta

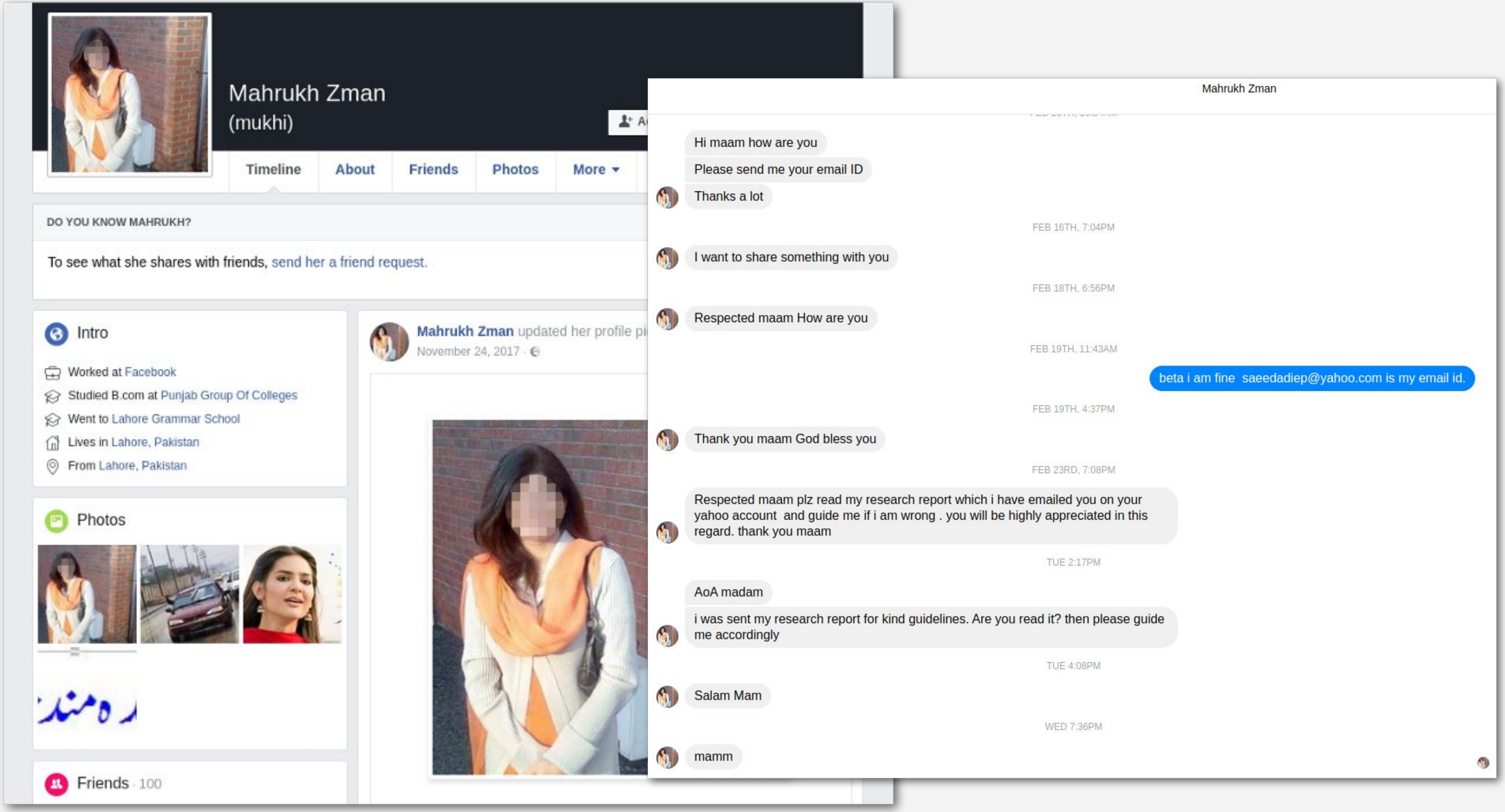
i am online

https://1drv.ms/u/s!Av3_DzkLYsevgUC4ngNC25AwoKVN

Chat with Raza docs.exe

Application

onedrive.live.com



Mahrukh Zman
(mukhi)

DO YOU KNOW MAHRUKH?

To see what she shares with friends, send her a friend request.

Intro

Worked at Facebook

Studied B.com at Punjab Group Of Colleges

Went to Lahore Grammar School

Lives in Lahore, Pakistan

From Lahore, Pakistan

Photos

Friends · 100

Mahrukh Zman updated her profile pi
November 24, 2017 ·

Mahrukh Zman

Hi maam how are you

Please send me your email ID

Thanks a lot

FEB 16TH, 7:04PM

I want to share something with you

FEB 18TH, 6:56PM

Respected maam How are you

FEB 19TH, 11:43AM

beta i am fine saeedadiep@yahoo.com is my email id.

FEB 19TH, 4:37PM

Thank you maam God bless you

FEB 23RD, 7:08PM

Respected maam plz read my research report which i have emailed you on your yahoo account and guide me if i am wrong . you will be highly appreciated in this regard. thank you maam

TUE 2:17PM

AoA madam

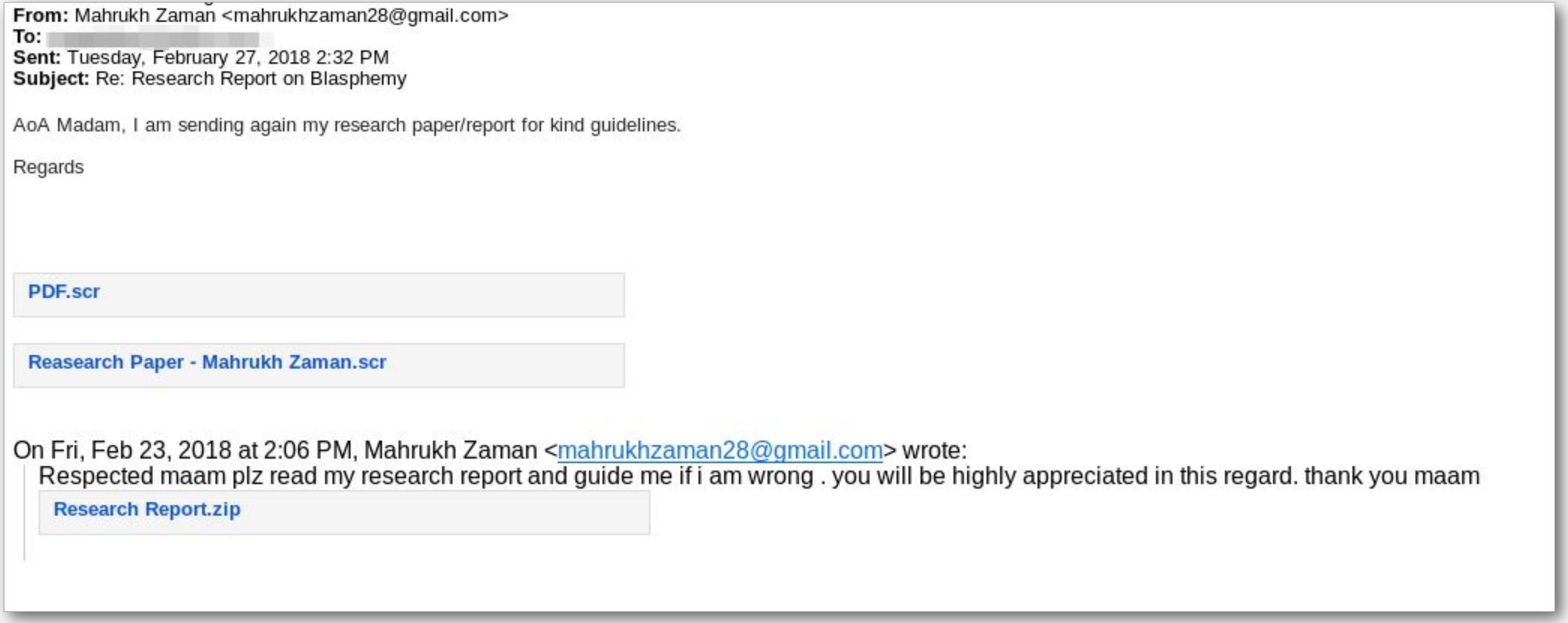
i was sent my research report for kind guidelines. Are you read it? then please guide me accordingly

TUE 4:08PM

Salam Mam

WED 7:36PM

mamm



From: Mahrukh Zaman <mahrukhzaman28@gmail.com>
To: [redacted]
Sent: Tuesday, February 27, 2018 2:32 PM
Subject: Re: Research Report on Blasphemy

AoA Madam, I am sending again my research paper/report for kind guidelines.

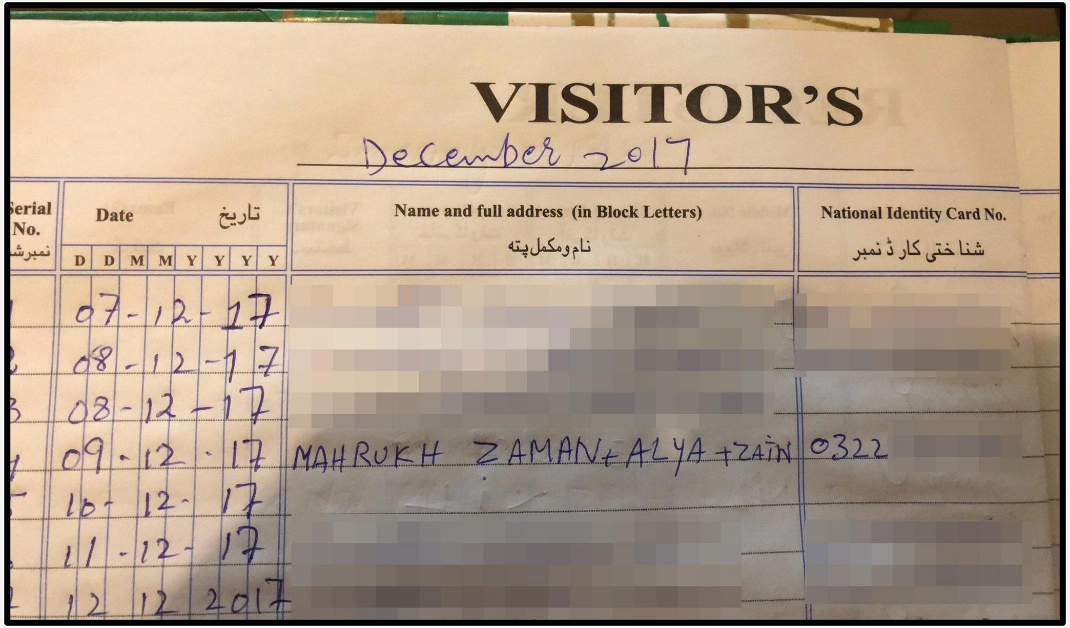
Regards

PDF.scr

Reasearch Paper - Mahrukh Zaman.scr

On Fri, Feb 23, 2018 at 2:06 PM, Mahrukh Zaman <mahrukhzaman28@gmail.com> wrote:

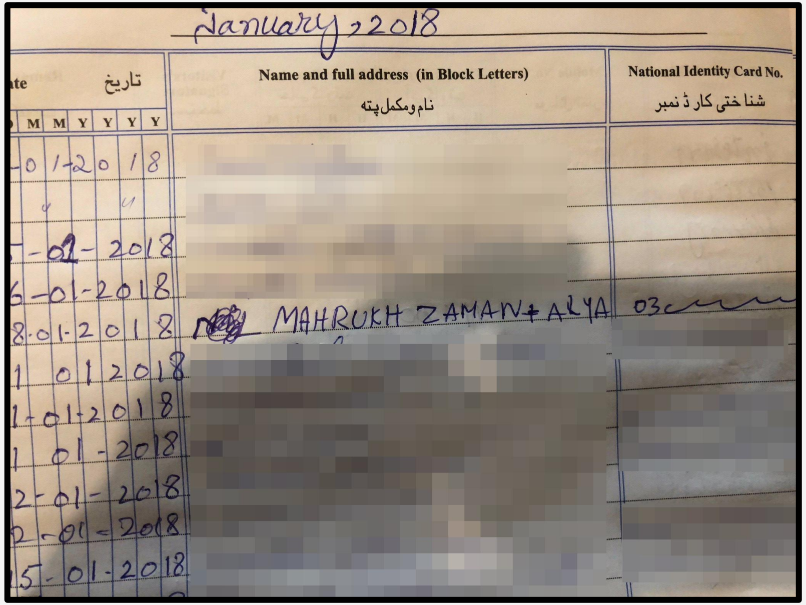
> Respected maam plz read my research report and guide me if i am wrong . you will be highly appreciated in this regard. thank you maam
>
> **Research Report.zip**



VISITOR'S

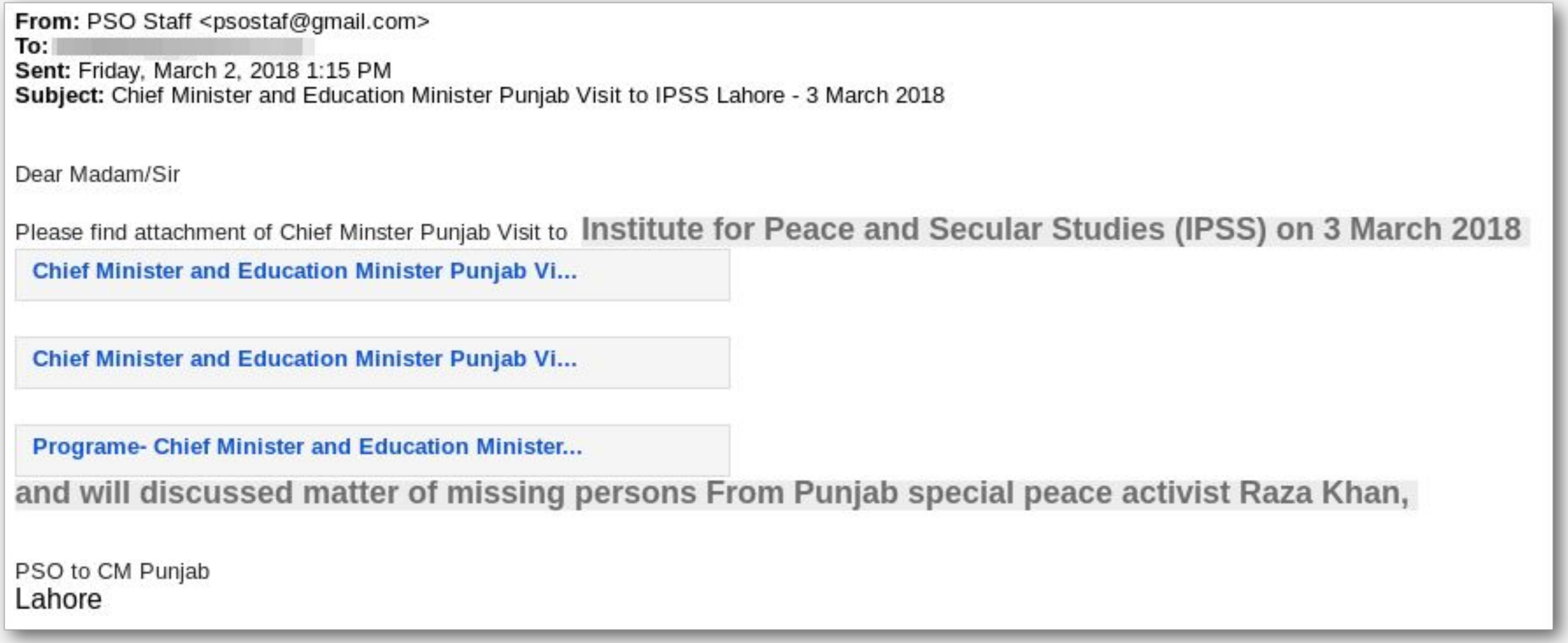
December 2017

Serial No. نمبرشمار	Date تاریخ D D M M Y Y Y Y	Name and full address (in Block Letters) نام ومکمل پتہ	National Identity Card No. شناختی کارڈ نمبر
1	07-12-17	[redacted]	[redacted]
2	08-12-17	[redacted]	[redacted]
3	08-12-17	[redacted]	
4	09-12-17	MAHRUKH ZAMAN+ALYA+ZAIN	0322 [redacted]
5	10-12-17		
	11-12-17	[redacted]	[redacted]
	12 12 2017	[redacted]	[redacted]



January, 2018

ate تاریخ M M Y Y Y Y	Name and full address (in Block Letters) نام ومکمل پتہ	National Identity Card No. شناختی کارڈ نمبر
-01-2018	[redacted]	
" "	[redacted]	
-01-2018	[redacted]	
6-01-2018	[redacted]	
8-01-2018	MAHRUKH ZAMAN+ALYA	03
1 01 2018	[redacted]	[redacted]
1-01-2018	[redacted]	[redacted]
1 01-2018	[redacted]	[redacted]
2-01-2018	[redacted]	[redacted]
2-01-2018	[redacted]	[redacted]
5-01-2018	[redacted]	[redacted]



From: PSO Staff <psostaf@gmail.com>
To: [redacted]
Sent: Friday, March 2, 2018 1:15 PM
Subject: Chief Minister and Education Minister Punjab Visit to IPSS Lahore - 3 March 2018

Dear Madam/Sir

Please find attachment of Chief Minster Punjab Visit to **Institute for Peace and Secular Studies (IPSS) on 3 March 2018**

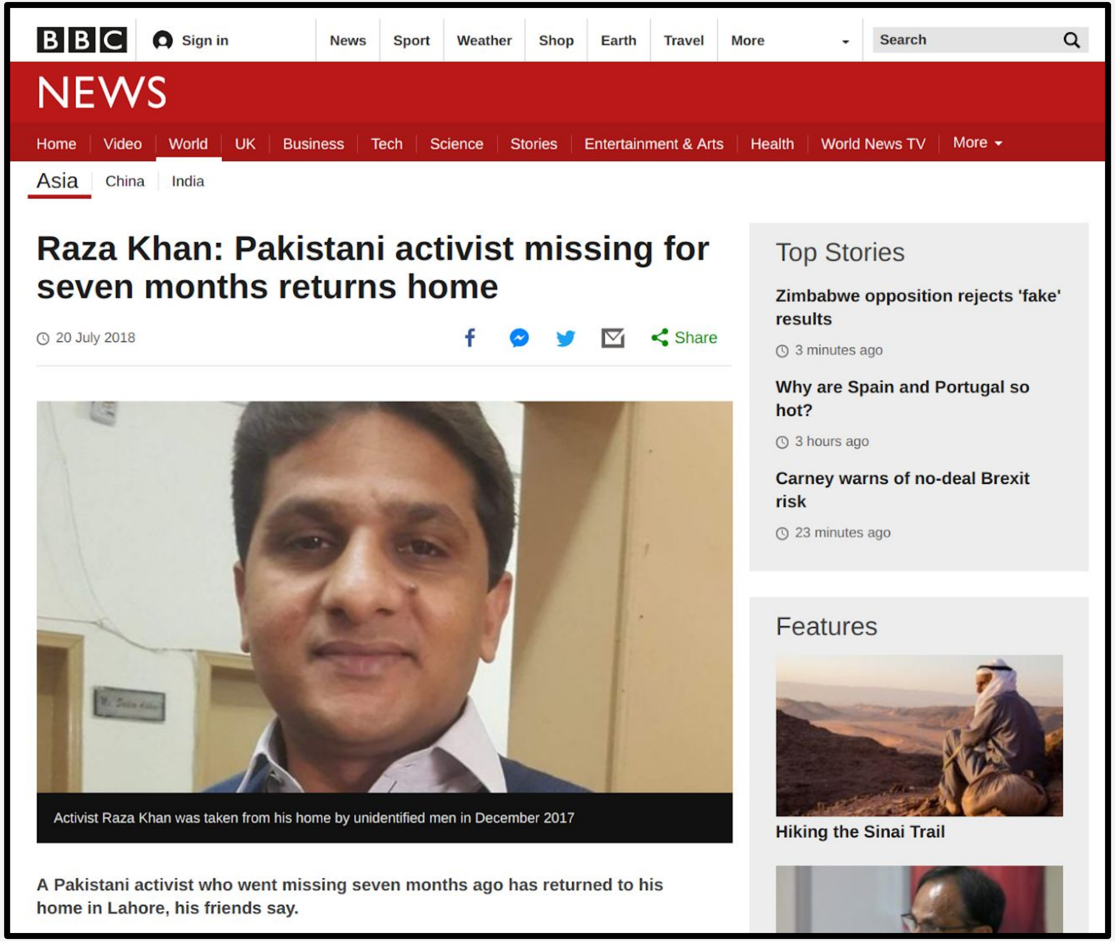
Chief Minister and Education Minister Punjab Vi...

Chief Minister and Education Minister Punjab Vi...

Programe- Chief Minister and Education Minister...

and will discussed matter of missing persons From Punjab special peace activist Raza Khan,

PSO to CM Punjab
Lahore



Raza Khan: Pakistani activist missing for seven months returns home

20 July 2018

Activist Raza Khan was taken from his home by unidentified men in December 2017

A Pakistani activist who went missing seven months ago has returned to his home in Lahore, his friends say.

Top Stories

Zimbabwe opposition rejects 'fake' results

3 minutes ago

Why are Spain and Portugal so hot?

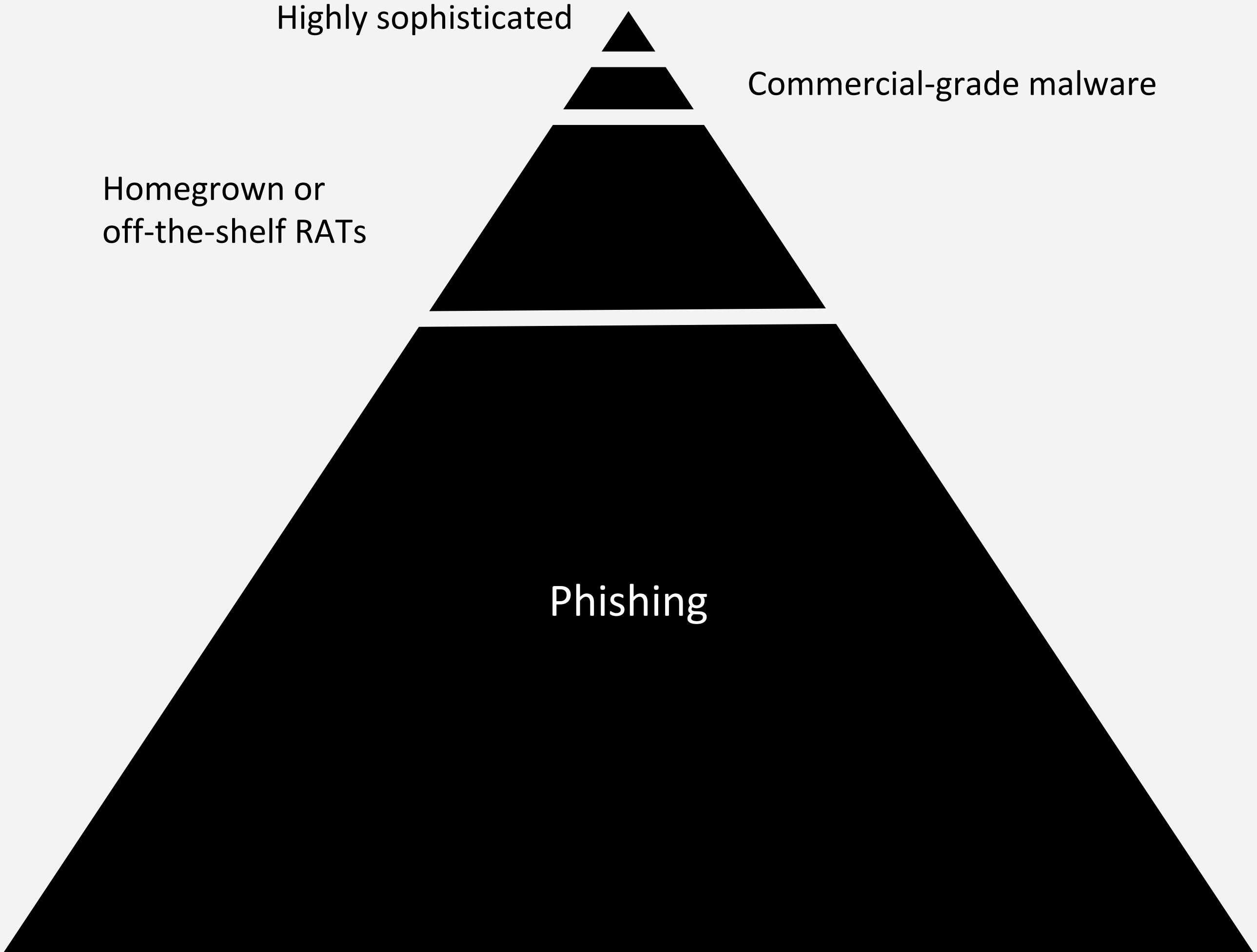
3 hours ago

Carney warns of no-deal Brexit risk

23 minutes ago

Features

Hiking the Sinai Trail



Highly sophisticated

Commercial-grade malware

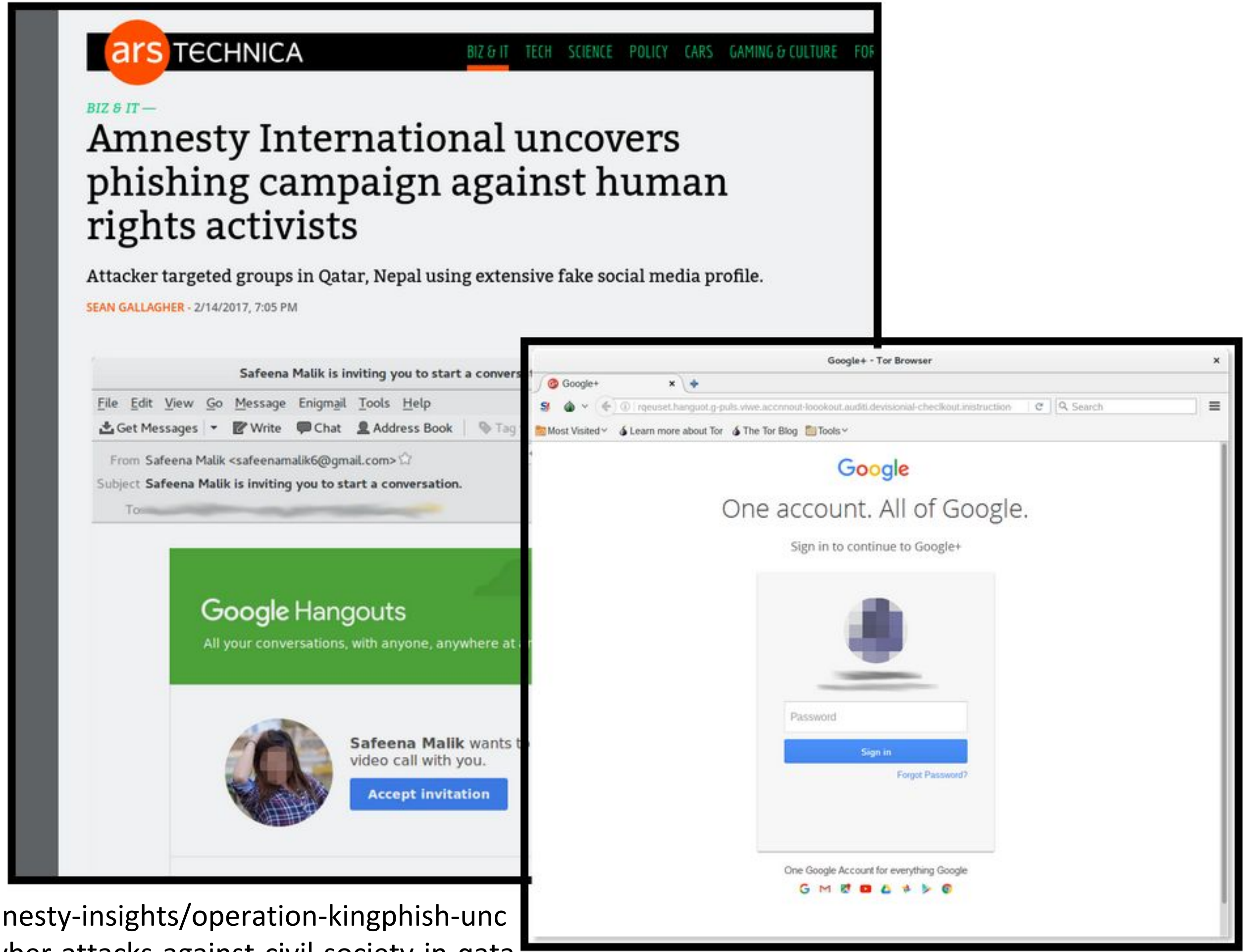
Homegrown or
off-the-shelf RATs

Phishing

Online harassment, deanonymization, intimidation, disinformation, DDoS, censorship, Internet shutdowns, etc.

Phishing is going strong

- Phishing is the most common threat.
- We see single ***targeted*** phishing campaigns going after individuals in the **hundreds** or **thousands**.



BIZ & IT —

Amnesty International uncovers phishing campaign against human rights activists

Attacker targeted groups in Qatar, Nepal using extensive fake social media profile.

SEAN GALLAGHER - 2/14/2017, 7:05 PM

Safeena Malik is inviting you to start a convers

From Safeena Malik <safeenamalik6@gmail.com>

Subject Safeena Malik is inviting you to start a conversation.

To [redacted]

Google Hangouts

All your conversations, with anyone, anywhere at

Safeena Malik wants t video call with you.

Google+ - Tor Browser

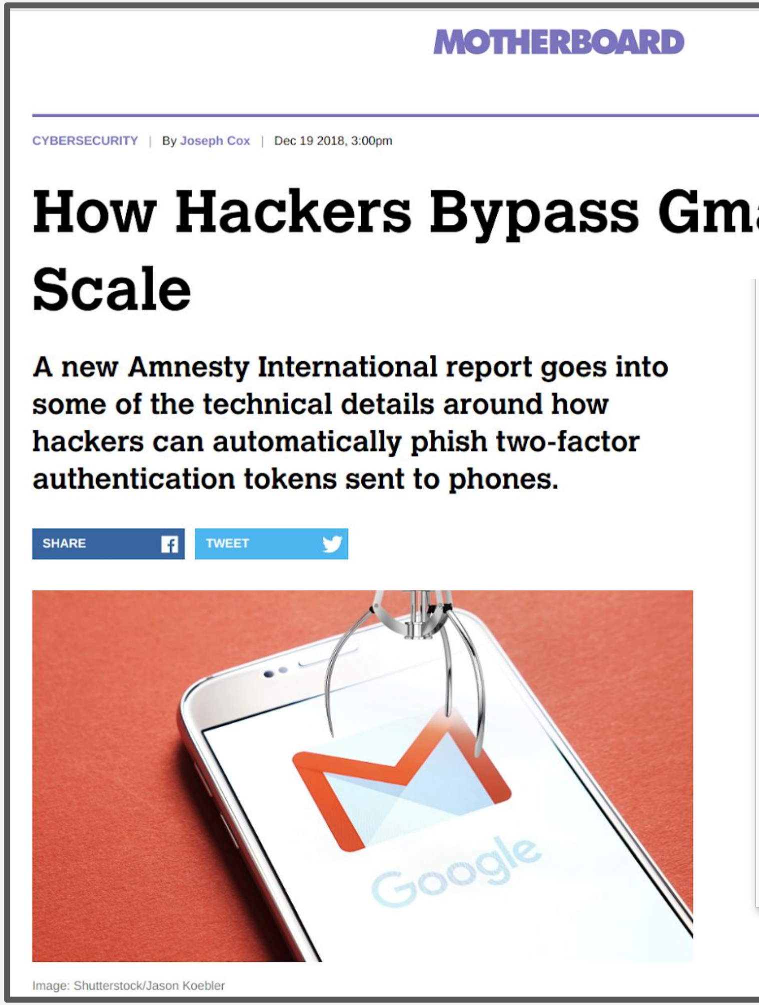
Google+
rqeuset.hanguot.g-puls.viwe.accnnout-loookout.auditi.devisionial-checlkout.inistruction
Search
Most Visited
Learn more about Tor
The Tor Blog
Tools
Google

One account. All of Google.

Sign in to continue to Google+

One Google Account for everything Google

https://medium.com/amnesty-insights/operation-kingphish-uncovering-a-campaign-of-cyber-attacks-against-civil-society-in-qatar-and-aa40c9e08852



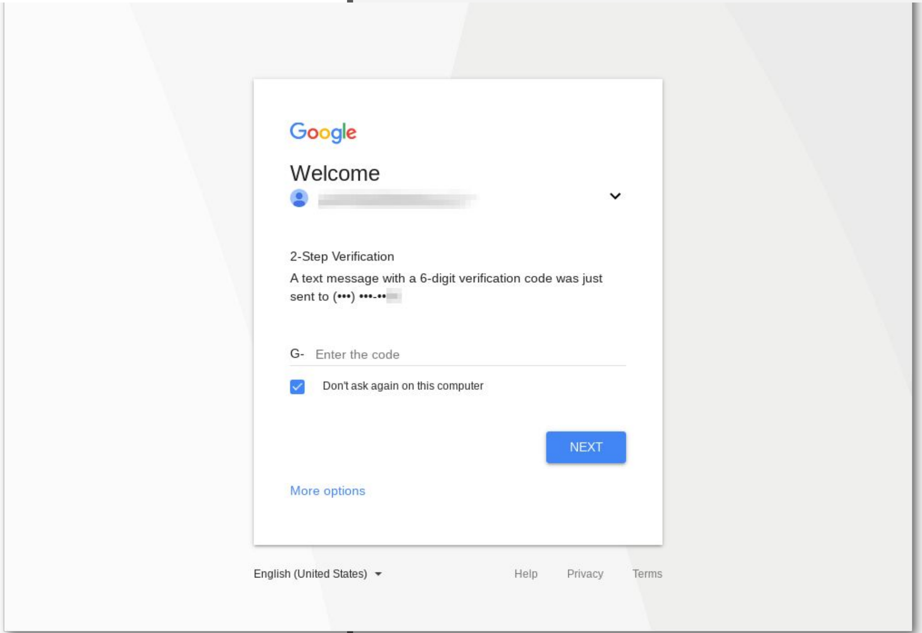
MOTHERBOARD

CYBERSECURITY | By Joseph Cox | Dec 19 2018, 3:00pm

How Hackers Bypass Gmail 2FA at Scale

A new Amnesty International report goes into some of the technical details around how hackers can automatically phish two-factor authentication tokens sent to phones.

Image: Shutterstock/Jason Koebler



Google

Welcome

[redacted]

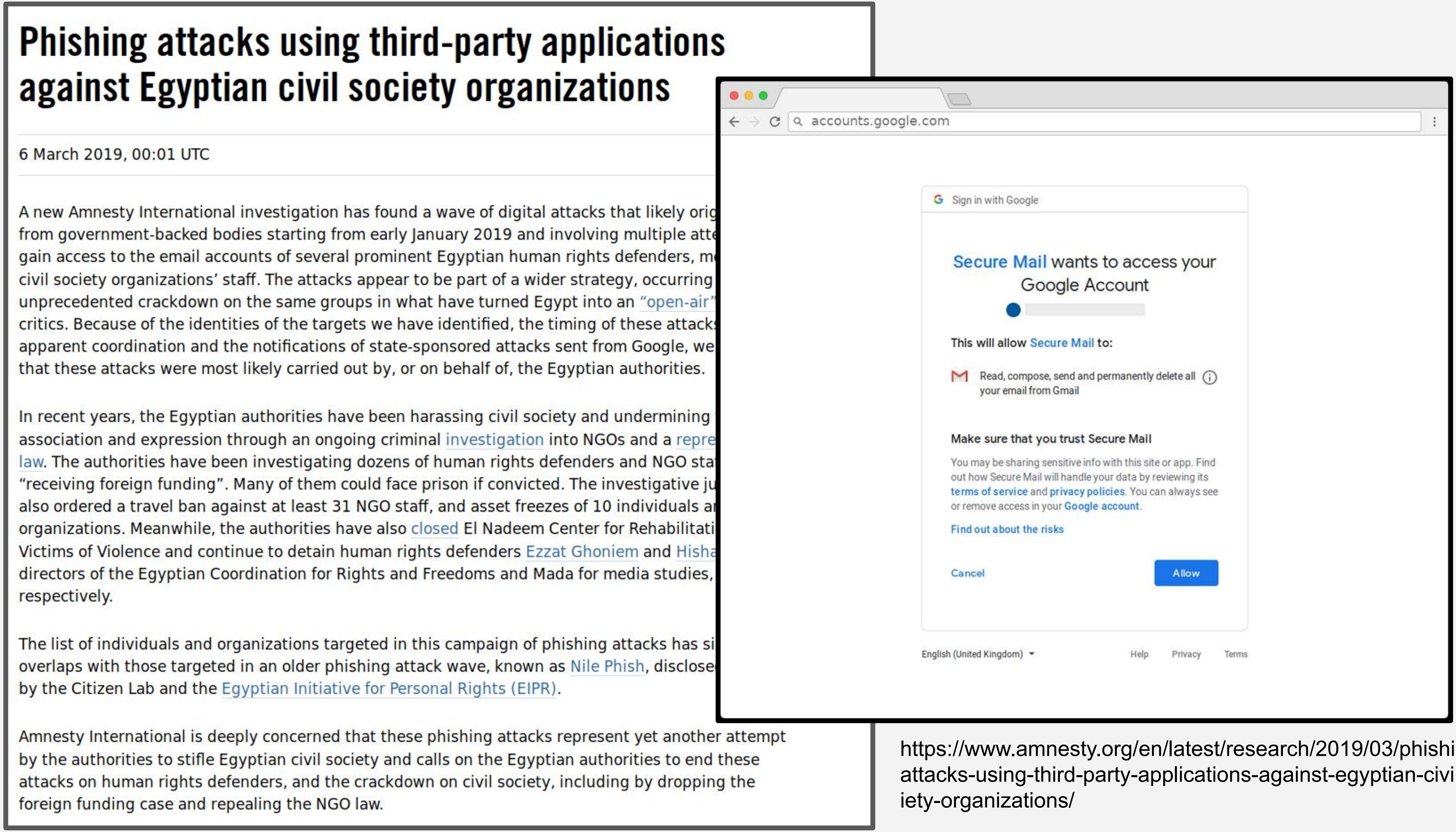
2-Step Verification

A text message with a 6-digit verification code was just sent to (•••) •••-••[redacted]

G- Enter the code

☑ Don't ask again on this computer

https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough/



Phishing attacks using third-party applications against Egyptian civil society organizations

6 March 2019, 00:01 UTC

A new Amnesty International investigation has found a wave of digital attacks that likely orig
from government-backed bodies starting from early January 2019 and involving multiple atte
gain access to the email accounts of several prominent Egyptian human rights defenders, m
civil society organizations' staff. The attacks appear to be part of a wider strategy, occurring
unprecedented crackdown on the same groups in what have turned Egypt into an "open-air"
critics. Because of the identities of the targets we have identified, the timing of these attack
apparent coordination and the notifications of state-sponsored attacks sent from Google, we
that these attacks were most likely carried out by, or on behalf of, the Egyptian authorities.

In recent years, the Egyptian authorities have been harassing civil society and undermining
association and expression through an ongoing criminal investigation into NGOs and a repre
law. The authorities have been investigating dozens of human rights defenders and NGO sta
"receiving foreign funding". Many of them could face prison if convicted. The investigative ju
also ordered a travel ban against at least 31 NGO staff, and asset freezes of 10 individuals a
organizations. Meanwhile, the authorities have also closed El Nadeem Center for Rehabilitati
Victims of Violence and continue to detain human rights defenders Ezzat Ghoniem and Hisha
directors of the Egyptian Coordination for Rights and Freedoms and Mada for media studies,
respectively.

The list of individuals and organizations targeted in this campaign of phishing attacks has si
overlaps with those targeted in an older phishing attack wave, known as Nile Phish, disclose
by the Citizen Lab and the Egyptian Initiative for Personal Rights (EIPR).

Amnesty International is deeply concerned that these phishing attacks represent yet another attempt by the authorities to stifle Egyptian civil society and calls on the Egyptian authorities to end these attacks on human rights defenders, and the crackdown on civil society, including by dropping the foreign funding case and repealing the NGO law.

accounts.google.com

Secure Mail wants to access your Google Account

This will allow Secure Mail to:

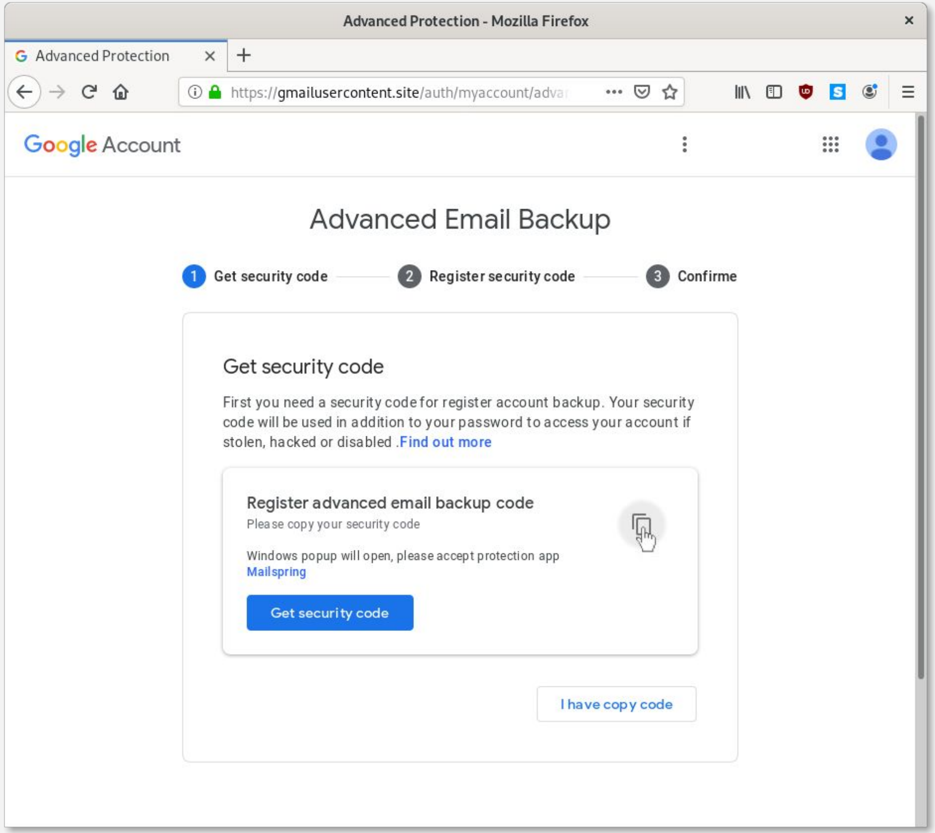
Read, compose, send and permanently delete all your email from Gmail

Make sure that you trust Secure Mail

You may be sharing sensitive info with this site or app. Find out how Secure Mail will handle your data by reviewing its terms of service and privacy policies. You can always see or remove access in your Google account.

Find out about the risks

https://www.amnesty.org/en/latest/research/2019/03/phishing-attacks-using-third-party-applications-against-egyptian-civil-society-organizations/



Advanced Protection - Mozilla Firefox

https://gmailusercontent.site/auth/myaccount/adva

Advanced Email Backup

1 Get security code —— 2 Register security code —— 3 Confirme

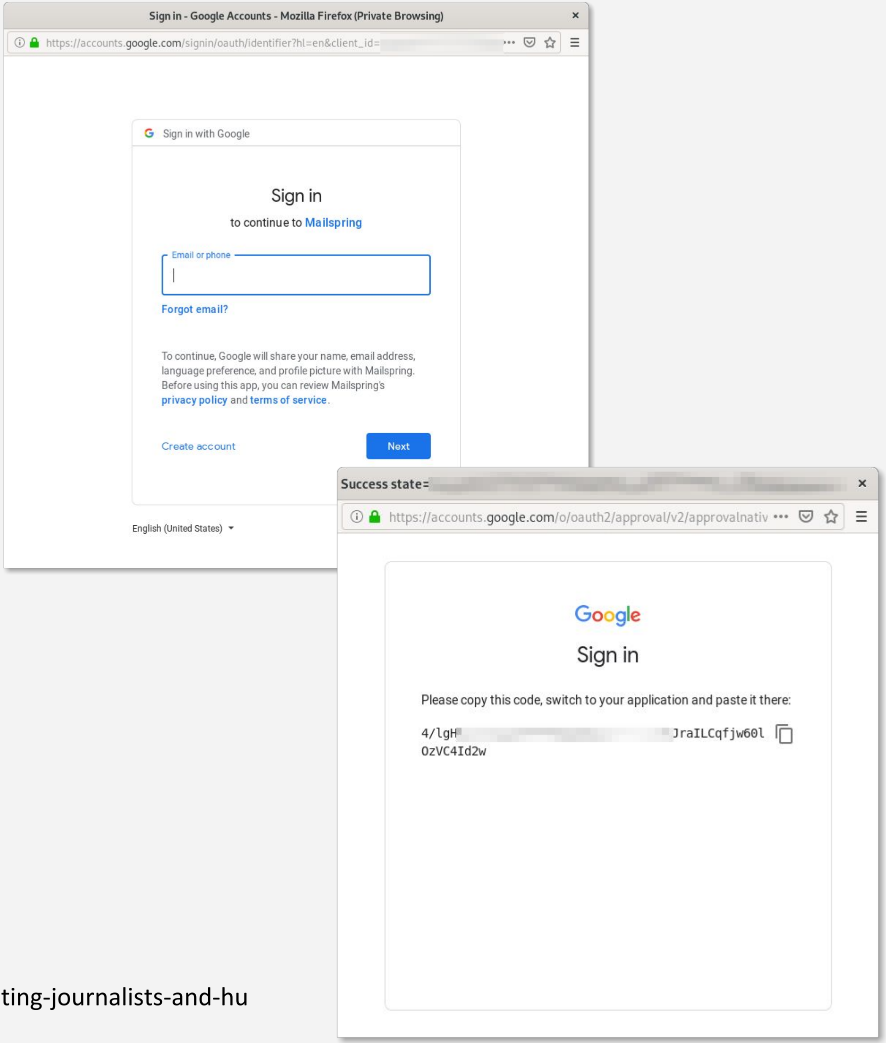
Get security code

First you need a security code for register account backup. Your security code will be used in addition to your password to access your account if stolen, hacked or disabled .Find out more

Register advanced email backup code

Please copy your security code

Windows popup will open, please accept protection app Mailspring



Sign in - Google Accounts - Mozilla Firefox (Private Browsing)

https://accounts.google.com/signin/oauth/identifier?hl=en&client_id=[redacted]

Sign in with Google

Sign in

to continue to Mailspring

Email or phone

To continue, Google will share your name, email address, language preference, and profile picture with Mailspring. Before using this app, you can review Mailspring's privacy policy and terms of service.

Success state=[redacted]

https://accounts.google.com/o/oauth2/approval/v2/approvalnativ

Google

Sign in

Please copy this code, switch to your application and paste it there:

4/lgH[redacted]JraILCqfjw60l
0zVC4Id2w

https://www.amnesty.org/en/latest/research/2019/08/evolving-phishing-attacks-targeting-journalists-and-human-rights-defenders-from-the-middle-east-and-north-africa/

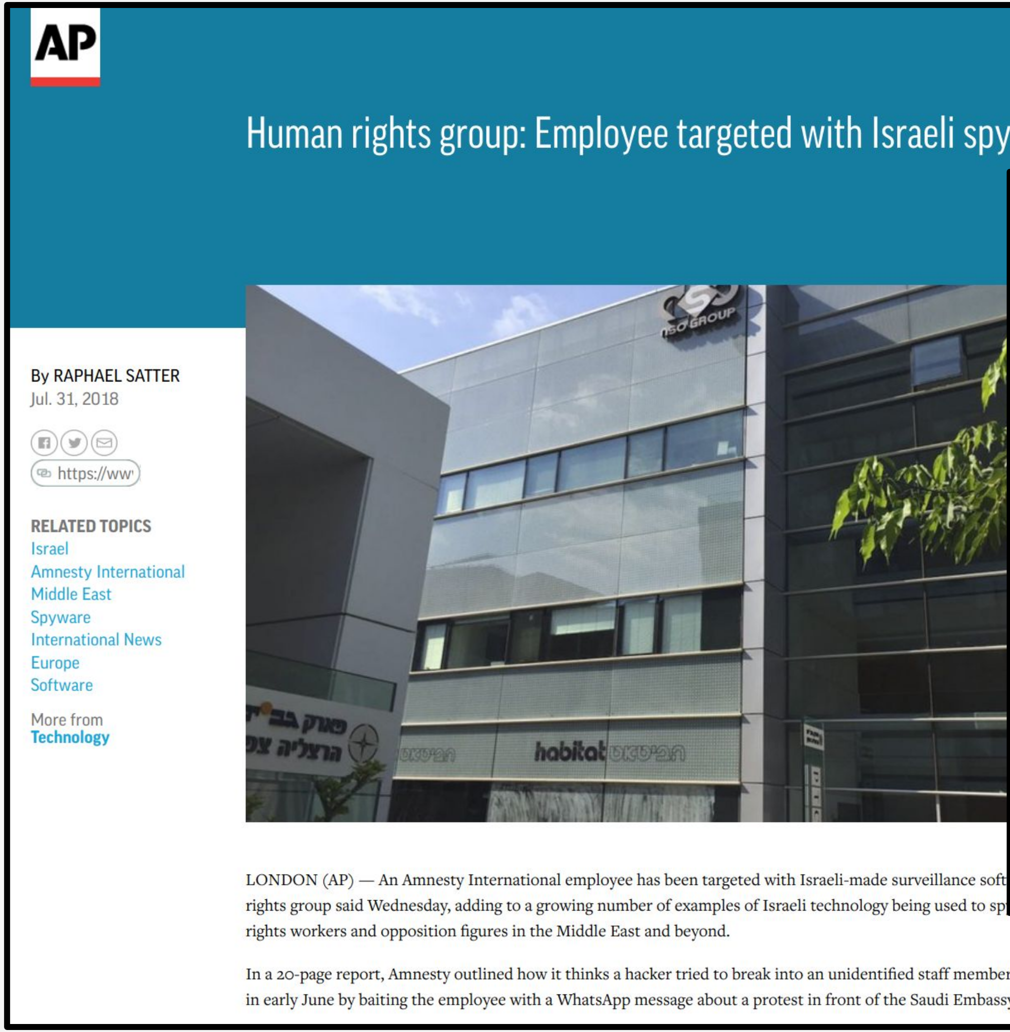
Shift in Phishing tactics

- There’s a shift in phishing tactics...
- **2FA phishing** becoming mainstream.
- **OAuth phishing** seeing a comeback.
- We are also starting to see **reverse proxies** getting adopted…
- **U2F** adoption is low - we are at an **inflection point** attackers are taking advantage of.

What about malware?

- Windows malware less predominant than 5-6 years ago. Mostly **PowerShell**, **VBScript** and commercial-grade penetration testing tools.
- Android malware on the rise, especially in certain areas.

- Generally a big gap of sophistication.



AP

Human rights group: Employee targeted with Israeli spyware

By RAPHAEL SATTER
Jul. 31, 2018

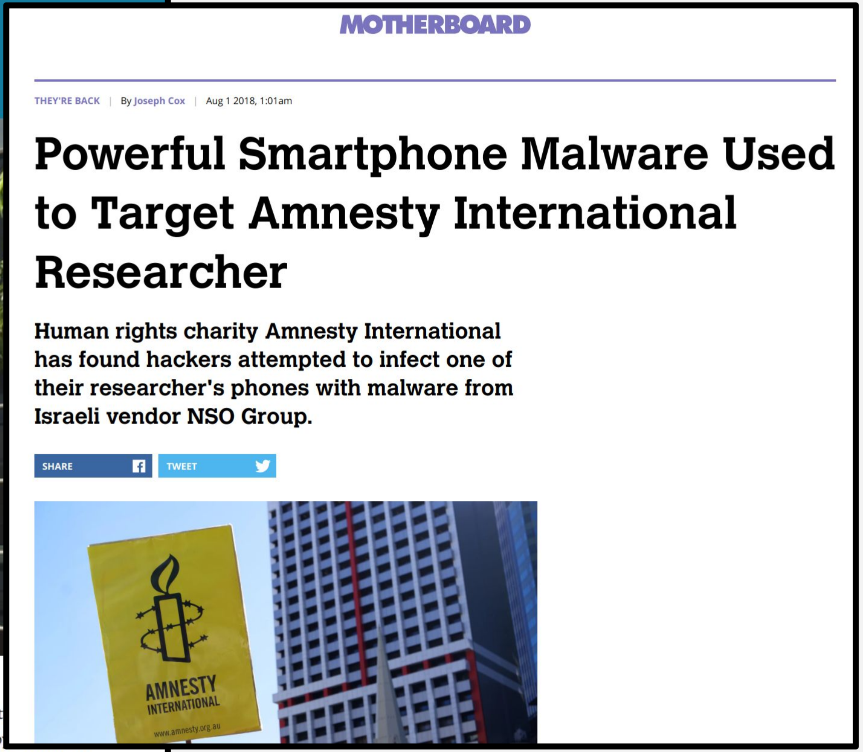
https://ww

RELATED TOPICS
Israel
Amnesty International
Middle East
Spyware
International News
Europe
Software

More from
Technology

LONDON (AP) — An Amnesty International employee has been targeted with Israeli-made surveillance soft rights group said Wednesday, adding to a growing number of examples of Israeli technology being used to sp rights workers and opposition figures in the Middle East and beyond.

In a 20-page report, Amnesty outlined how it thinks a hacker tried to break into an unidentified staff member's smartphone in early June by baiting the employee with a WhatsApp message about a protest in front of the Saudi Embassy in Washington.



MOTHERBOARD

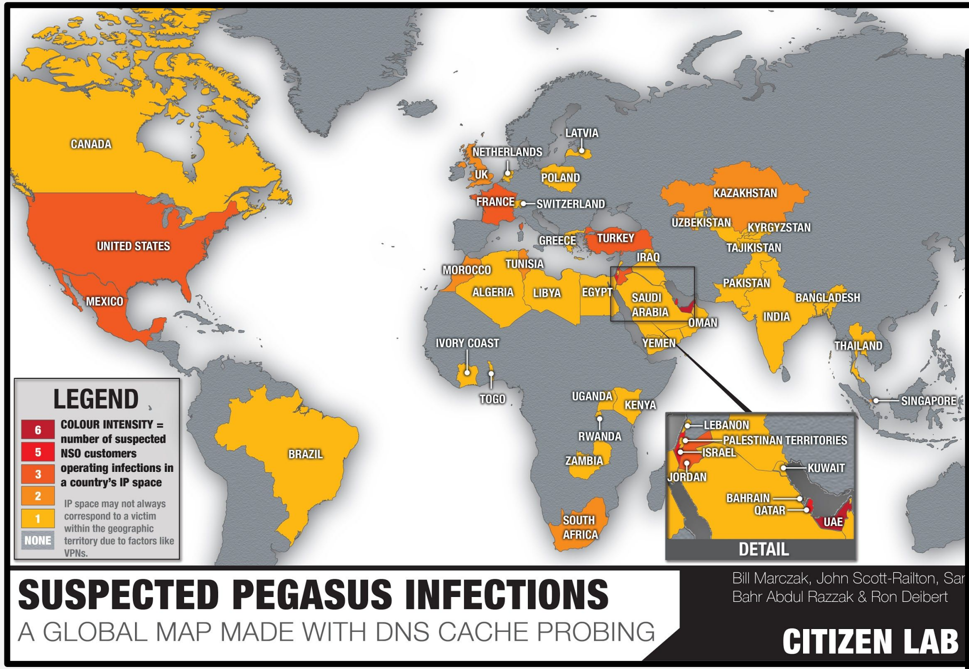
THEY'RE BACK | By Joseph Cox | Aug 1 2018, 1:01am

Powerful Smartphone Malware Used to Target Amnesty International Researcher

Human rights charity Amnesty International has found hackers attempted to infect one of their researcher's phones with malware from Israeli vendor NSO Group.

SHARE TWEET

https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/

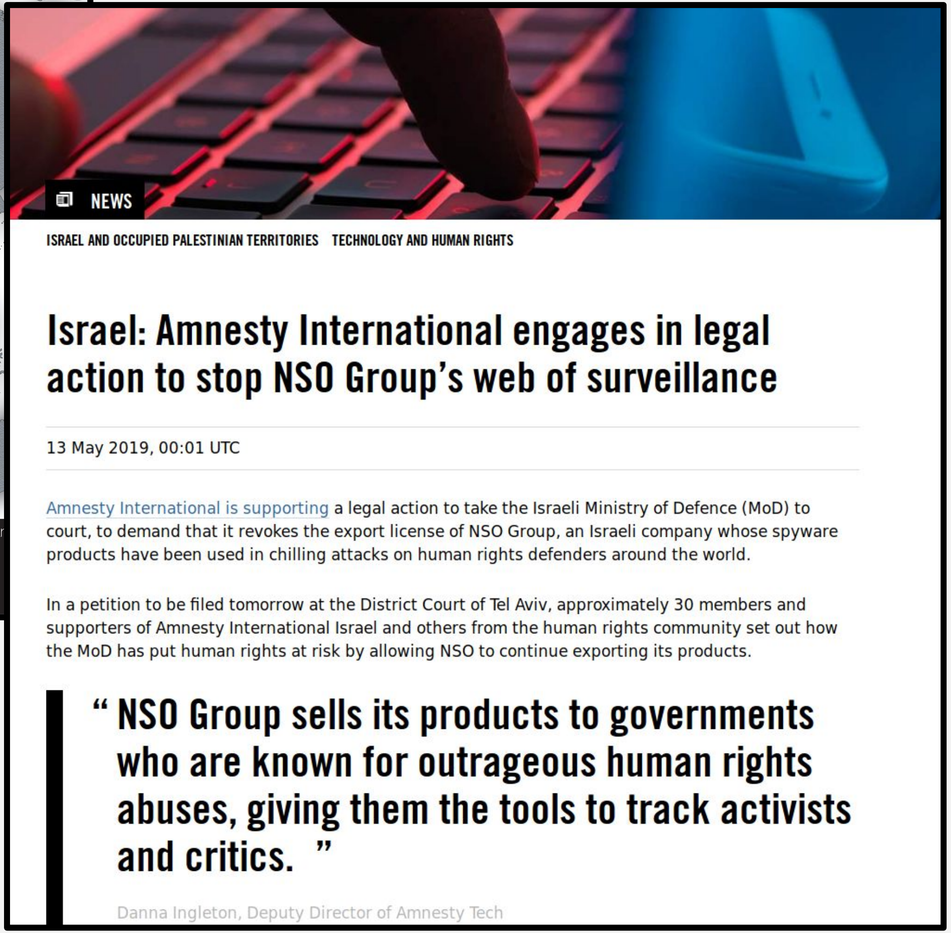


SUSPECTED PEGASUS INFECTIONS

A GLOBAL MAP MADE WITH DNS CACHE PROBING

Bill Marczak, John Scott-Railton, Sar
Bahr Abdul Razzak & Ron Deibert

CITIZEN LAB



ISRAEL AND OCCUPIED PALESTINIAN TERRITORIES TECHNOLOGY AND HUMAN RIGHTS

Israel: Amnesty International engages in legal action to stop NSO Group's web of surveillance

13 May 2019, 00:01 UTC

Amnesty International is supporting a legal action to take the Israeli Ministry of Defence (MoD) to court, to demand that it revokes the export license of NSO Group, an Israeli company whose spyware products have been used in chilling attacks on human rights defenders around the world.

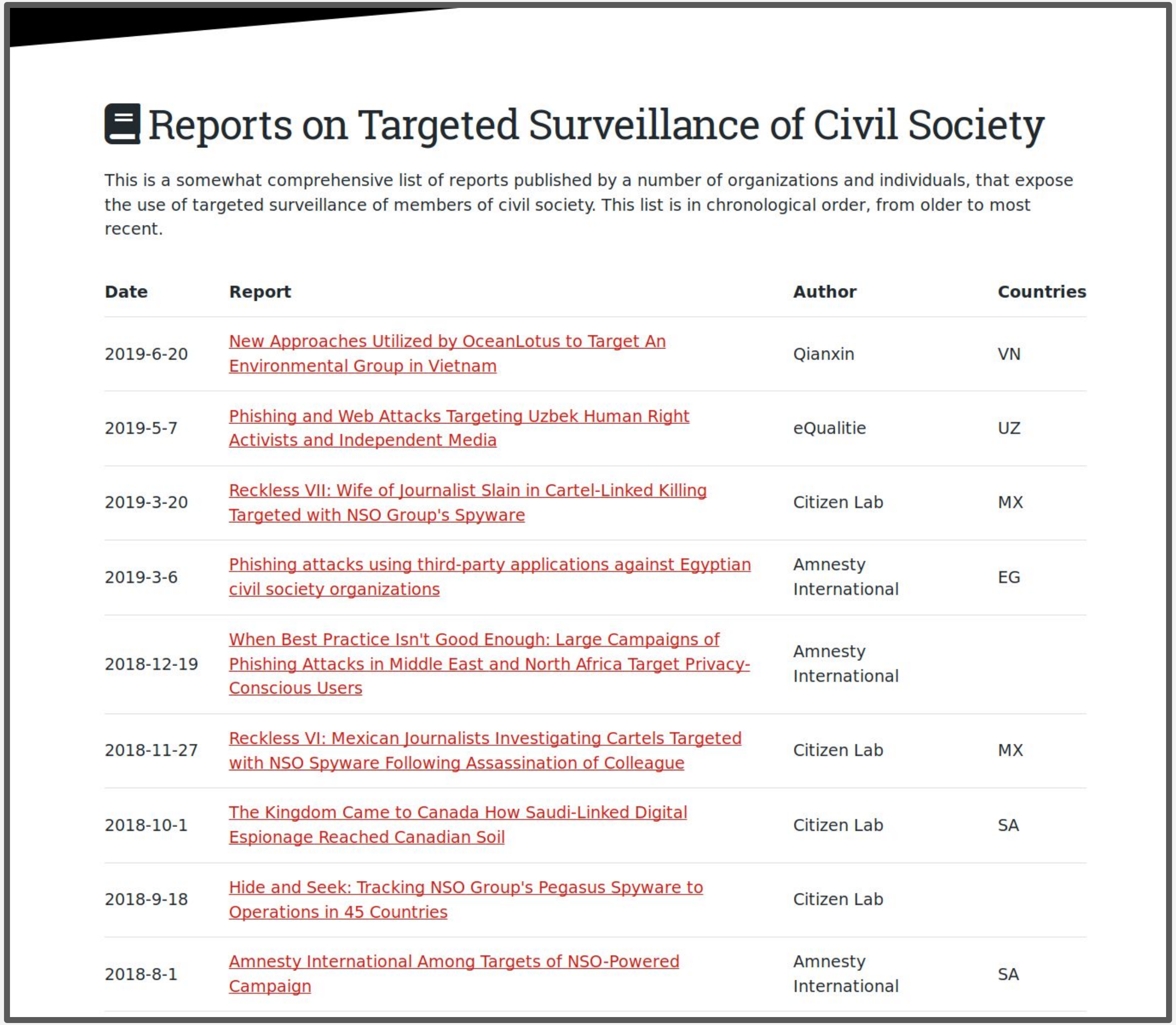
In a petition to be filed tomorrow at the District Court of Tel Aviv, approximately 30 members and supporters of Amnesty International Israel and others from the human rights community set out how the MoD has put human rights at risk by allowing NSO to continue exporting its products.

> “ NSO Group sells its products to governments who are known for outrageous human rights abuses, giving them the tools to track activists and critics. ”
>
> Danna Ingleton, Deputy Director of Amnesty Tech

What’s coming next?

- I do believe **things are getting better**.
- Compared to when I started, successful infection of devices is a lot harder.
- Advancements in software and hardware security (especially on mobile) will make it increasingly harder in the future.
- **However, attackers don’t stop: they adapt.** They will pivot to different strategies and tactics, and find new entry points.
- Civil society’s adversaries do not operate in the digital realm only.

but...



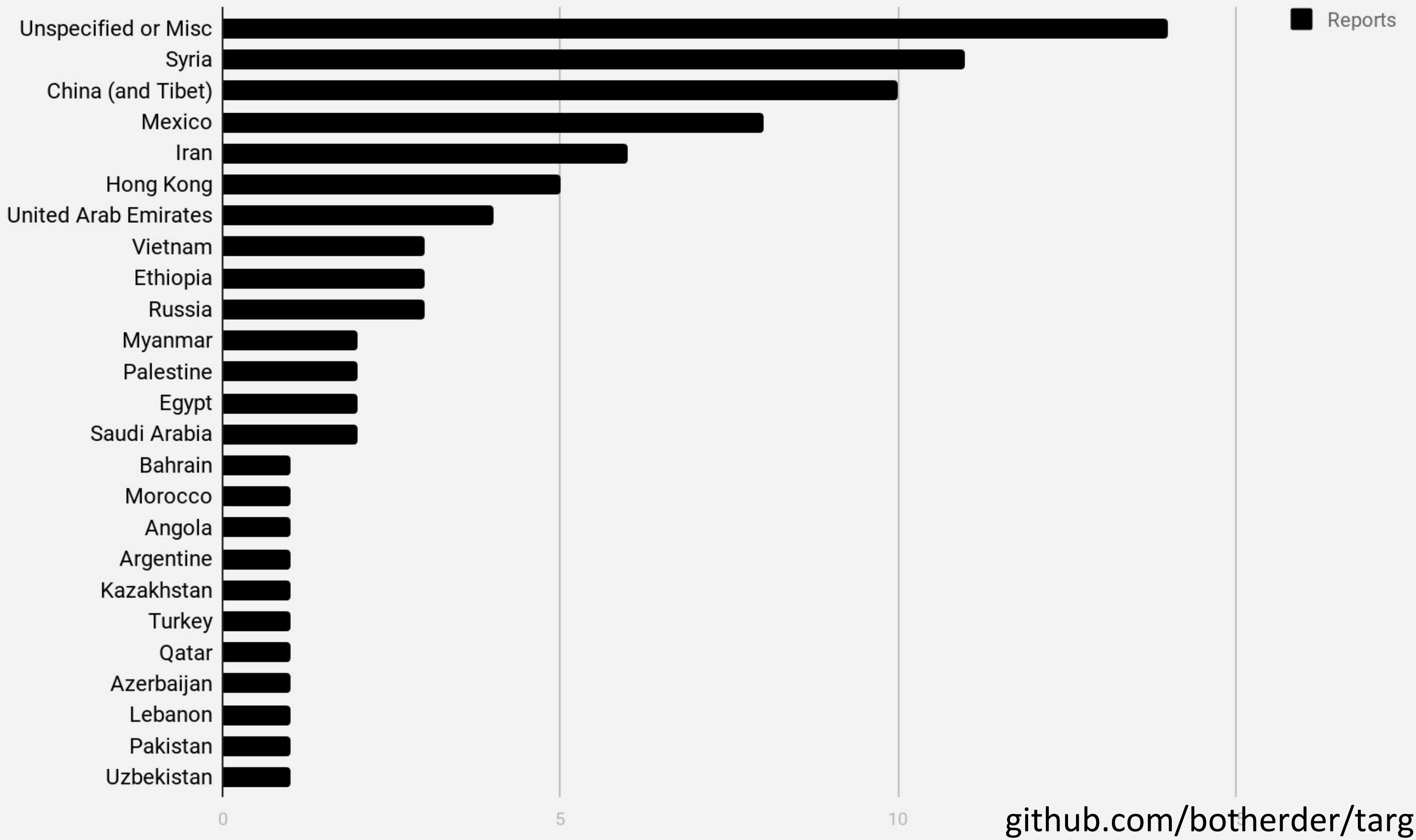
Reports on Targeted Surveillance of Civil Society

This is a somewhat comprehensive list of reports published by a number of organizations and individuals, that expose the use of targeted surveillance of members of civil society. This list is in chronological order, from older to most recent.

Date	Report	Author	Countries
2019-6-20	New Approaches Utilized by OceanLotus to Target An Environmental Group in Vietnam	Qianxin	VN
2019-5-7	Phishing and Web Attacks Targeting Uzbek Human Right Activists and Independent Media	eQualitie	UZ
2019-3-20	Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware	Citizen Lab	MX
2019-3-6	Phishing attacks using third-party applications against Egyptian civil society organizations	Amnesty International	EG
2018-12-19	When Best Practice Isn't Good Enough: Large Campaigns of Phishing Attacks in Middle East and North Africa Target Privacy-Conscious Users	Amnesty International	
2018-11-27	Reckless VI: Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague	Citizen Lab	MX
2018-10-1	The Kingdom Came to Canada How Saudi-Linked Digital Espionage Reached Canadian Soil	Citizen Lab	SA
2018-9-18	Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries	Citizen Lab	
2018-8-1	Amnesty International Among Targets of NSO-Powered Campaign	Amnesty International	SA

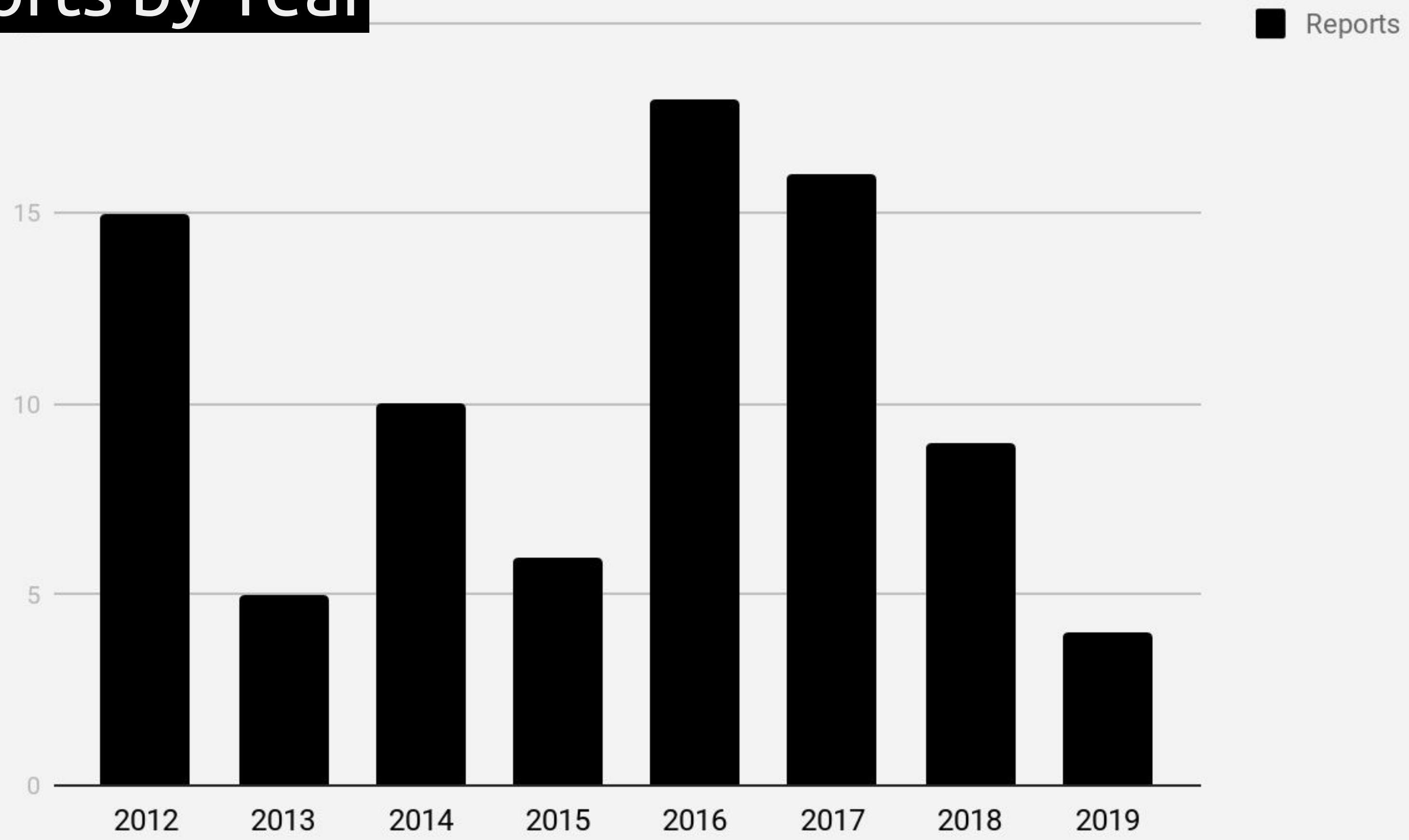
https://**securitywithoutborders.org/**resources/targeted-surveillance-reports.html

Reports by Country



github.com/botherder/targetedthreats

Reports by Year



github.com/botherder/targetedthreats

Challenges

Imbalance

Access to technology and security solutions

Threats faced

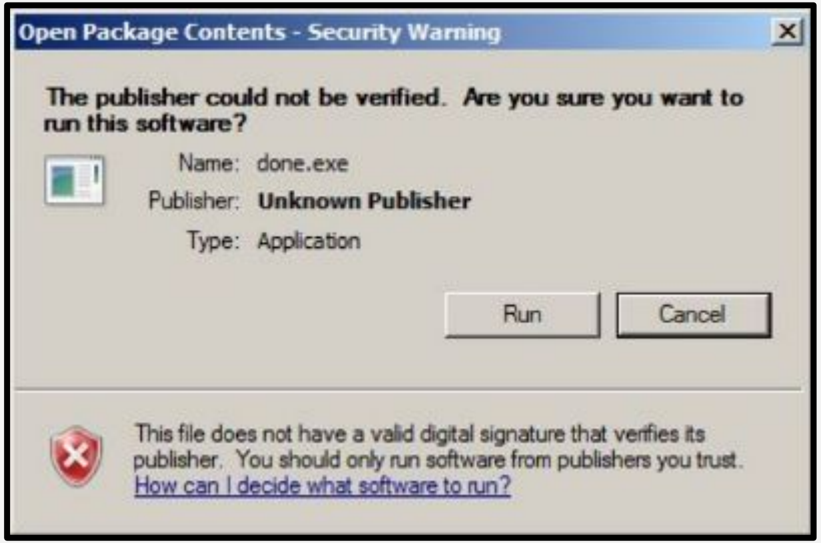
Civil society tends to be at the margins of conversations on cybersecurity.

Consumer vs. Enterprise

- Human rights defenders, journalists, dissidents, are normally **equipped with consumer-grade technology**.
- However, they face **enterprise-grade threats**.
  - Often, at a higher cost.
- They suffer from inadequate “default configurations”, and security features only available to corporate customers.

Some seem arbitrary

- Macros?
- PowerShell
- VBScript
- DDE links
- LNK launchers
- Embedding OLE objects



Open Package Contents - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: done.exe

Publisher: **Unknown Publisher**

Type: Application

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

Sometimes the *mitigations* are Security Warnings that imply some understanding of the system’s security features.

Some are more tricky

- Device Encryption vs. BitLocker
- Security hardening vs. inspectability of mobile devices.

“*Basic*” problems “*solved*” in the corporate space, are largely **unresolved** in civil society.

In civil society it is **hard to devise a unified security model**, even among groups or organisations.

Lack of control

- Different devices.
- Different platforms.
- Different services.
- Different networks.
- BYO*.

Lack of control

- Geographical distribution.
- Sometimes different laws (encryption?) and access to services (censorship or sanctions).

Lack of control

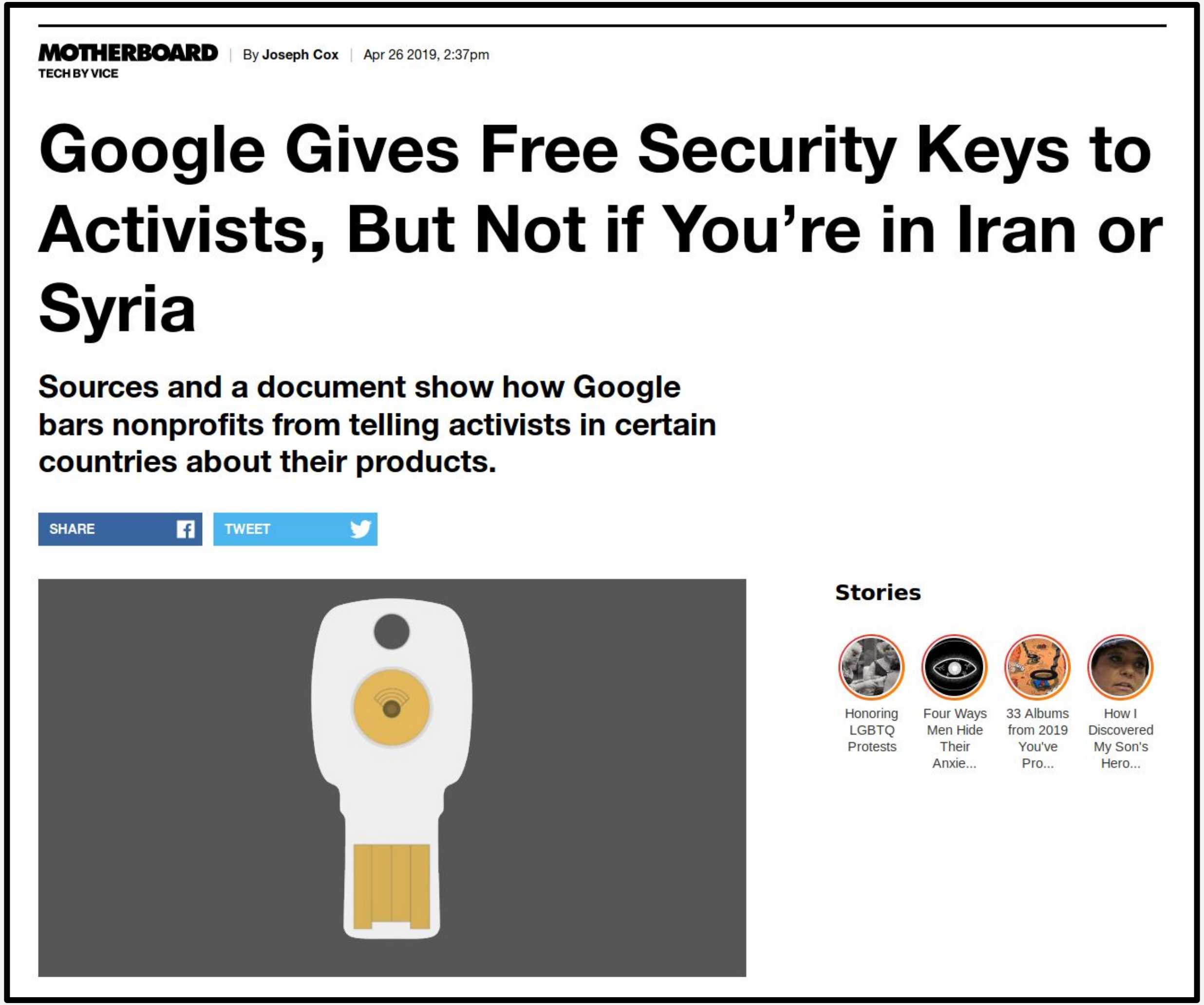
- Sometimes a shared email solution (e.g. GSuite).
- Often HRDs work under separate identities or using personal accounts.
  - e.g.: in some countries, having explicit contact with some NGOs can be problematic.

Human Rights Defenders have to be their own *IT*, *SOC* and *Incident Response*.

The burden to **do everything right** is so heavy, that eventually things will go horribly wrong.

Lack of resources

- Obviously, civil society does not have large resources.
- Often the few resources are badly spent.
  - Security culture and literature is very “*Western*”. Recommendations are not always relevant.
- Procuring technology can be difficult.
  - e.g. 700€ for an iPhone.
  - e.g. U2F tokens.



MOTHERBOARD
TECH BY VICE | By Joseph Cox | Apr 26 2019, 2:37pm

Google Gives Free Security Keys to Activists, But Not if You’re in Iran or Syria

Sources and a document show how Google bars nonprofits from telling activists in certain countries about their products.

SHARE
TWEET
Stories
Honoring LGBTQ Protests
Four Ways Men Hide Their Anxie...
33 Albums from 2019 You've Pro...
How I Discovered My Son's Hero...

Importance of detection

- Consumer security products generally focus on blind protection.
- **Contextualized detection** is extremely important.
  - e.g. an Antivirus blocks a malicious execution.
  - e.g. Gmail identifies an email as malicious and hides it in spam.
  - e.g. a phishing attack fails because of U2F.

Blocking an attack is important, but knowing of targeting helps with **risk calculation**.

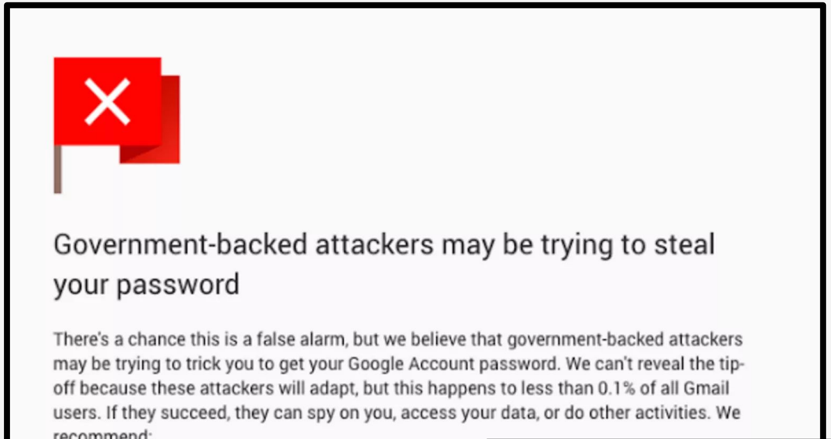
Hacking attempts might be a sign that it is time to leave, or not return home.

Opportunities

Canaries in the coalmine

Threat actors targeting corporates and governments are **often the same** actors targeting civil society. We observed domestic targeting anticipate the same tools & tactics later used against foreign states and corporates.

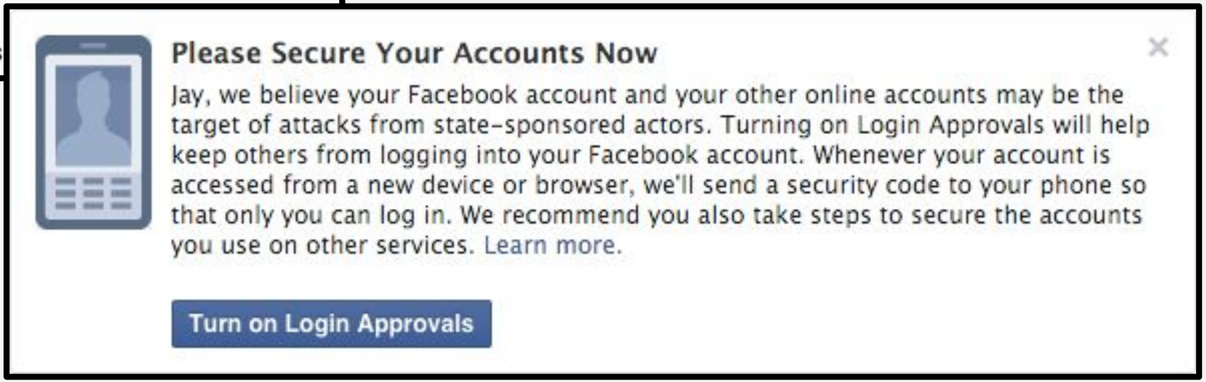
This cuts both ways



Government-backed attackers may be trying to steal your password

There's a chance this is a false alarm, but we believe that government-backed attackers may be trying to trick you to get your Google Account password. We can't reveal the tip-off because these attackers will adapt, but this happens to less than 0.1% of all Gmail users. If they succeed, they can spy on you, access your data, or do other activities. We recommend:

Enable two-factor authentication and s



Please Secure Your Accounts Now

Jay, we believe your Facebook account and your other online accounts may be the target of attacks from state-sponsored actors. Turning on Login Approvals will help keep others from logging into your Facebook account. Whenever your account is accessed from a new device or browser, we'll send a security code to your phone so that only you can log in. We recommend you also take steps to secure the accounts you use on other services. Learn more.

We need to do more and better!

If you work at a service provider, you almost surely have some at-risk individuals!

Creative security

- Because so much is missing, a lot can be done.
- Doing security in this area, means starting from the basics and think differently.
  - Talking to strangers and clicking on links is part of their work.
  - Different ecosystem than enterprise.
- Opportunity to be creative:
  - What could mitigations to phishing look like?
  - What could inspection and verification of infection look like?
  - How can we simplify triaging?
  - What services could be beneficial and how do we adapt them?

Getting involved?

- It’s not easy and there is no recipe.
- Speak to folks working in the sector.
- Contribute to existing projects and initiatives.
- Civil society organizations (even the big ones) desperately need talented security engineers. It can be a very frustrating, but humbling and gratifying job.
- Donate a bunch of U2F keys to your favorite organizations! ;)

Thank you!

Contacts

- **Work email:** nex@amnesty.org
- **PGP:** nex@nex.sx (0521 6F3B 8684 8A30 3C2F E37D D166 F166 7359 D880)
- **Newsletter:** https://nex.sx/newsletter/
- **Twitter (write-only):** @botherder