Digital Threat Landscape

GIJN Cyber Investigation Training - Week 3

$ whoami

- Infosec engineer by training, worked in the industry for several years
- In 2016, joined the Citizen Lab to research targeted surveillance of civil society
- Since then, I worked at Amnesty International investigating spyware attacks. Now working for Human Rights Watch
- Into nerdy Internet anecdotes, political history and tea

Who are you?

Today

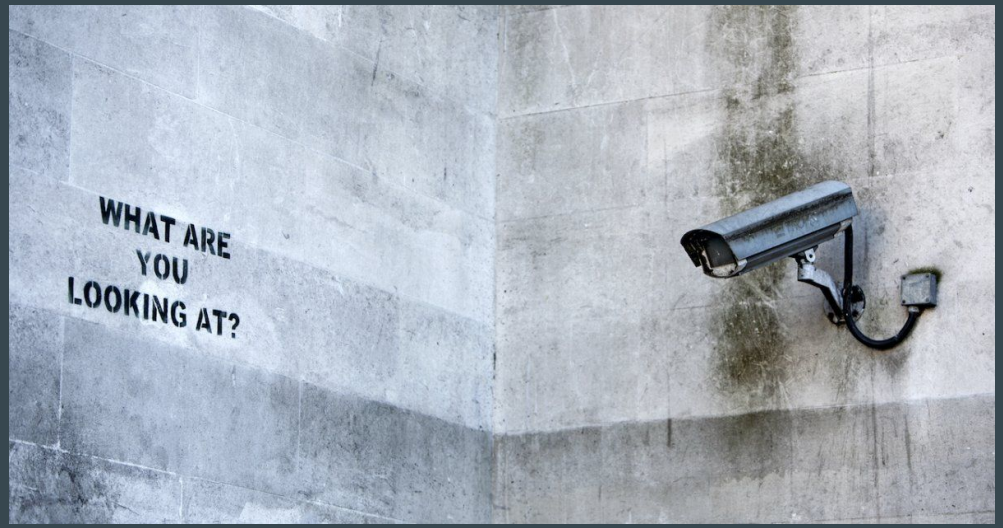
Let’s talk about Digital Surveillance :

- What is the landscape?
- How to investigate it?
- Different forms of digital surveillance
- Impact of digital surveillance
- Some 101 Digital Security Advices

What is Digital Surveillance?

What is Digital Surveillance?

- Digital surveillance is in every aspect of our life today
- Can be led by companies or by states, often both with shared interest



Let's take your phone

Wiretapping of phone calls

Bluetooth trackers

Trackers hidden in smartphone apps

Wifi Trackers

Data gathered by Google / Apple on the phone

Celltower informations

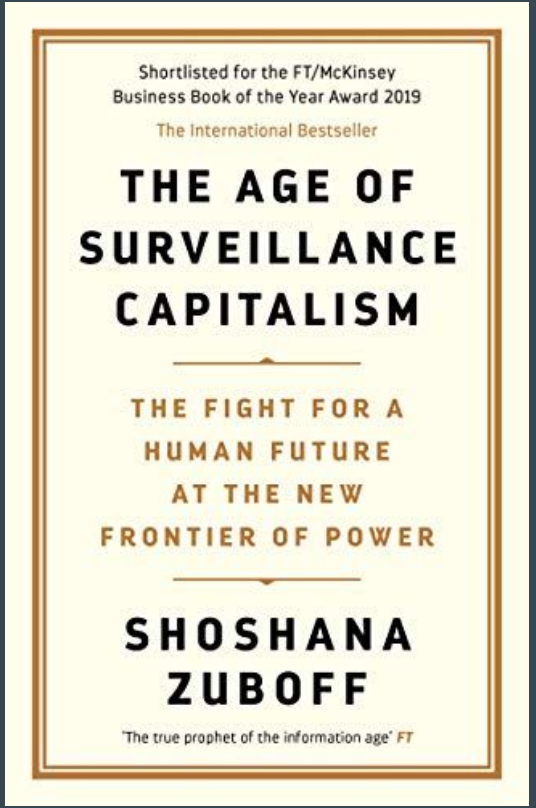
Cloud Synchronisation

Surveillance Capitalism

- Since the explosions of data, companies have understood that they can make money with user data

- “Data is the new oil”

- Most companies are collecting as much data as possible on their customers in order to generate revenues



Why do states carry out digital surveillance?

- Fight crime and all, but also, keep civil society under control

- Privacy is not only a right, but also a capacity for civil society to keep making the state accountable for its abuses

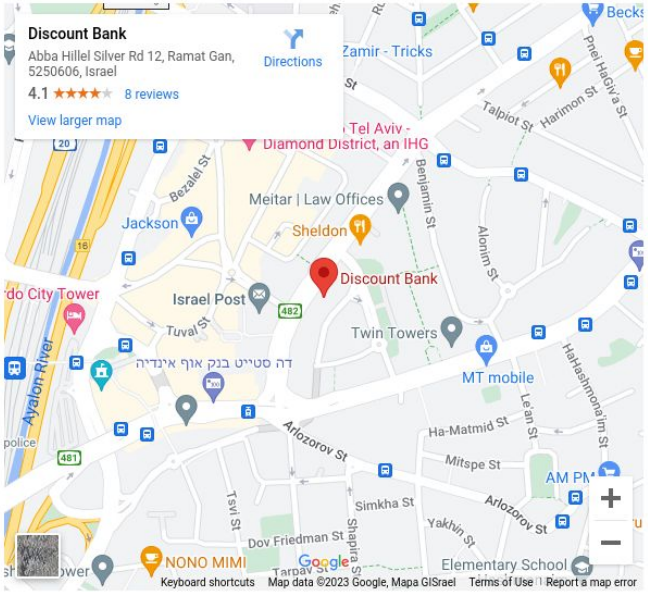
Investigating Digital Surveillance

Tracking the Surveillance Industry

- They want to hide but they need to exist

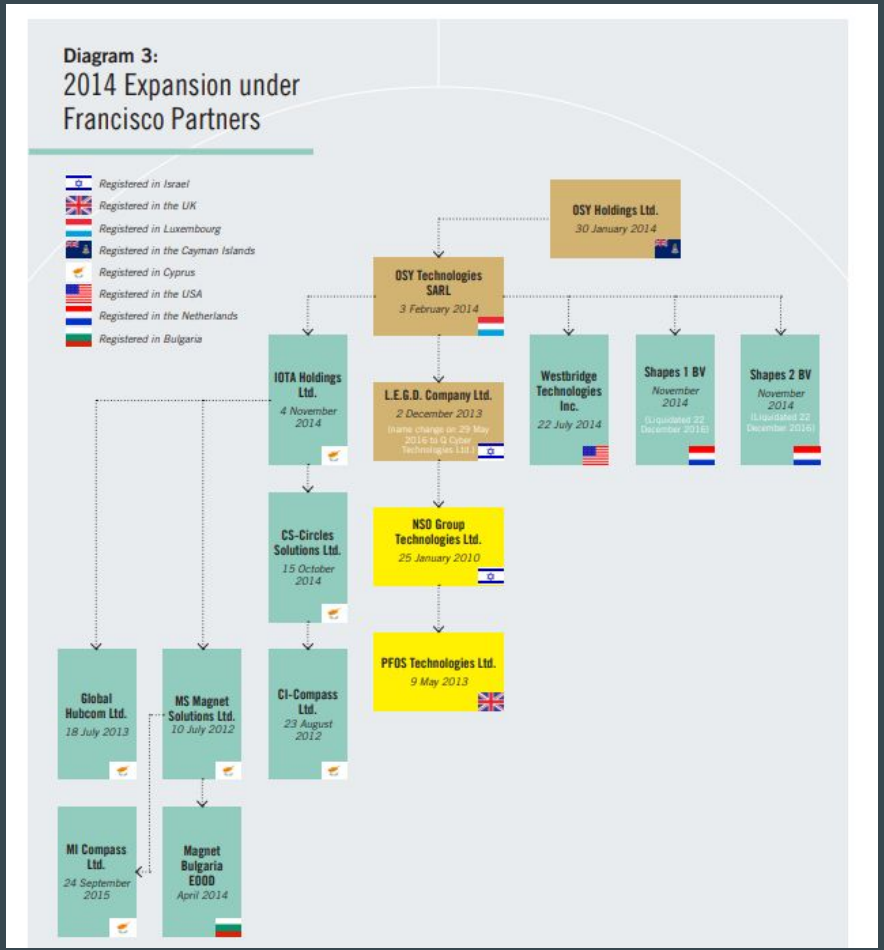
General Information

Company name	Squares Ltd.
Company name	QUADREAM LTD
Company number	515397651
Type of organization	Company
Type of corporation	Israeli private company
Company status	Active
Company objectives	To engage in any lawful business
Date of incorporation	08-02-2016
Government company	No
Restrictions	Limited
Last annual report (submitted)	2022
City	Ramat Gan
Street name	Drech Abba Hilel
House number	12
Postal Code	5250606
Country	Israel



Tracking the Surveillance Industry

- They want to hide but they need to exist

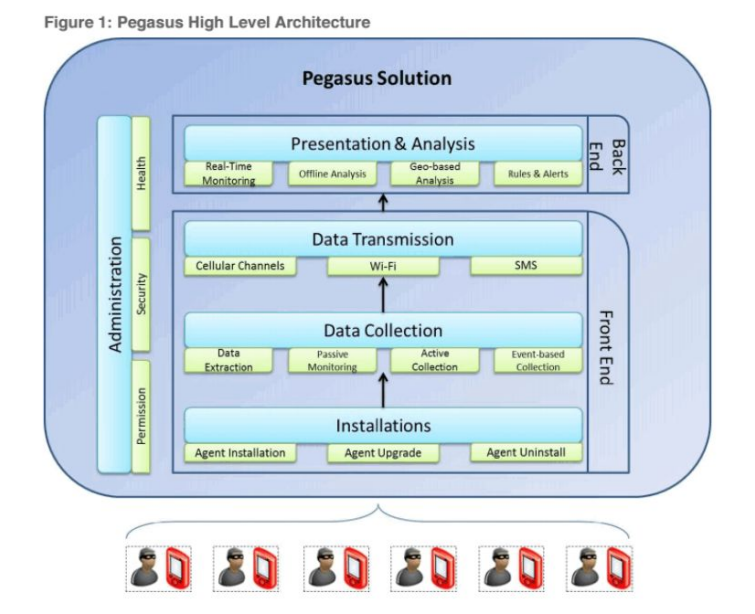


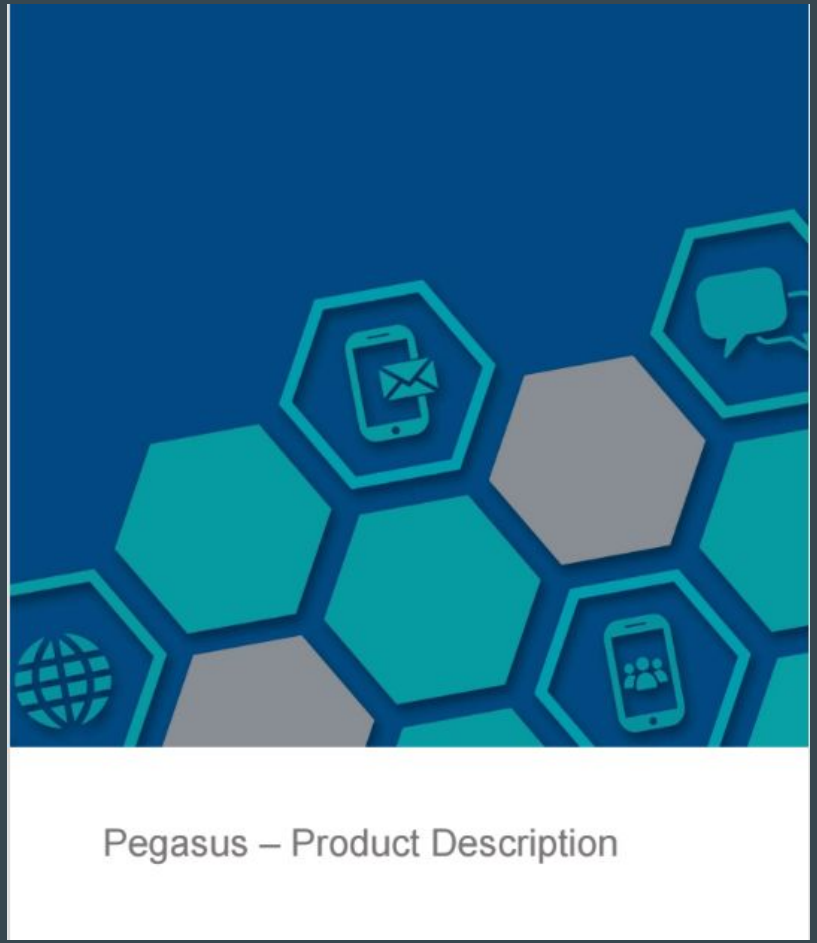
Tracking the Surveillance Industry

- They want to hide but they need to sell

Tracking the Surveillance Industry

- They want to hide but they need to sell





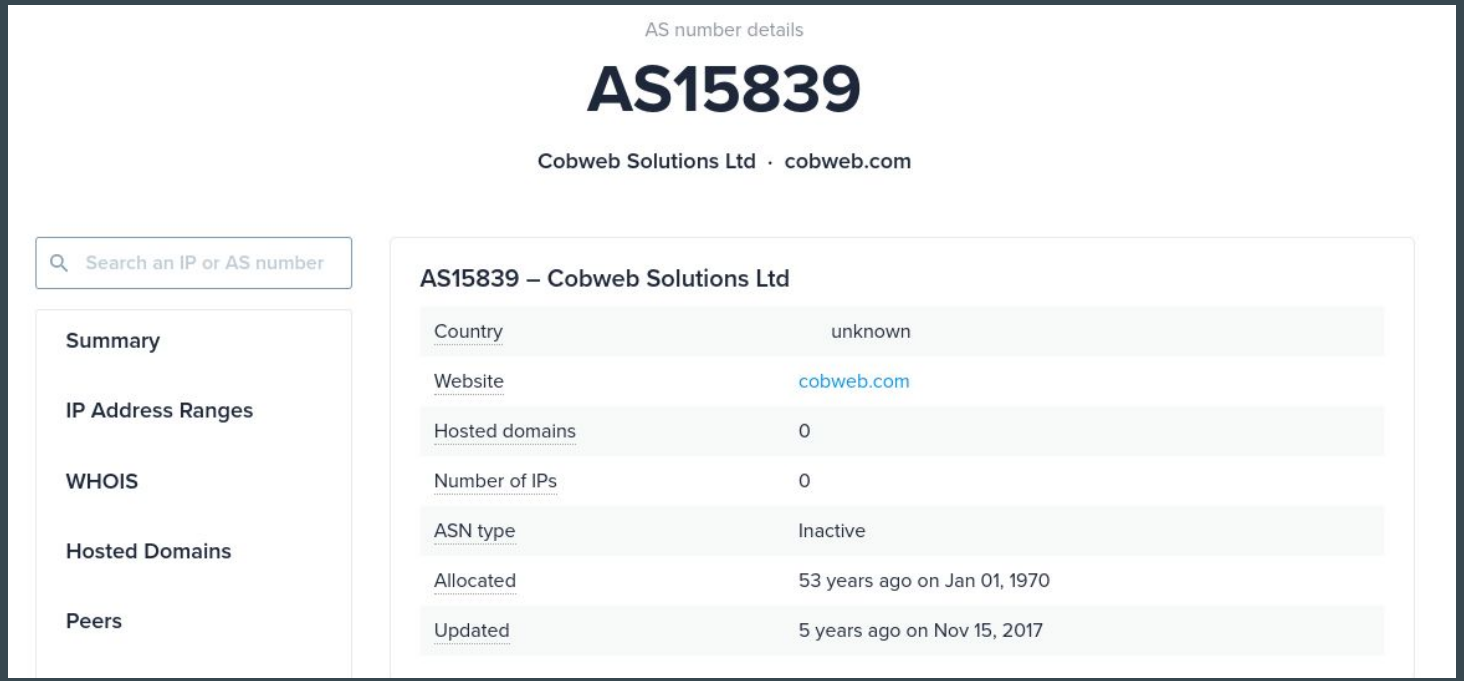
Tracking the Surveillance Industry

- They want to hide but they need to sell

http://www.sibat.mod.gov.il/defense/

Tracking the Surveillance Industry

- They want to hide but they need to run



Different Forms of Digital Surveillance

Phone network monitoring

- Oldest form of digital surveillance, owned by most countries

- Assume phone calls can be monitored by authorities of the country you are in

Phone Network Monitoring

The Government of South Sudan conducts communications surveillance with at least one type of equipment bought in Israel. Amnesty International found that, at least from March 2015 to February 2017, Israeli Verint Systems Ltd, a subsidiary of American Verint Systems Inc., through Vivacell Network of the World (henceforth Vivacell), provided the South Sudanese authorities, including the NSS, with communications interception equipment and annual support services. This is concerning because both South Sudan's legal framework governing surveillance and the Israeli export licencing regime are not in line with international human rights standards. The NSS can likely only intercept communications with collaboration from telecommunication service providers. Tapped telephone conversations have been presented as evidence in court, recounted to a detainee in interrogations, and appear to have provided leads for arbitrary arrests. The NSS also monitors media and social media and has used this information to arbitrarily arrest and illegally detain journalists and human rights defenders.

"THESE WALLS HAVE EARS"

THE CHILLING EFFECT OF SURVEILLANCE IN SOUTH SUDAN

AMNESTY INTERNATIONAL

https://www.amnesty.org/en/wp-content/uploads/2022/10/AFR6535772021ENGLISH.pdf

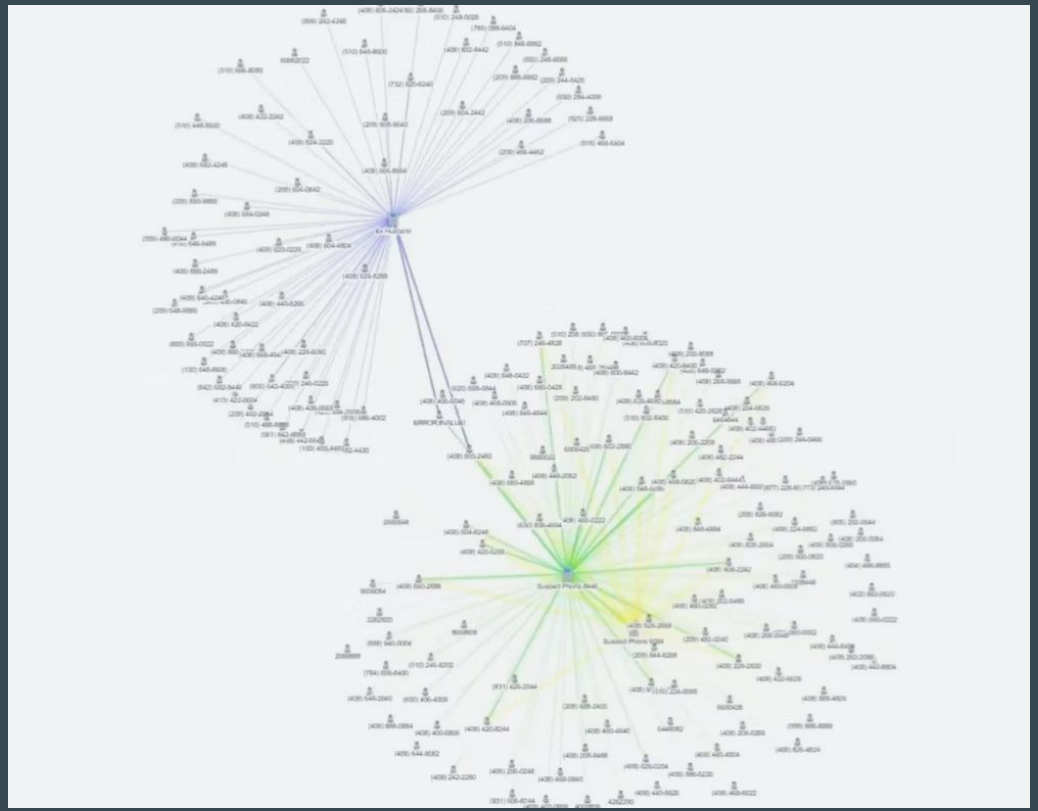
Celltower dump

- Cell towers contains traces of location of all the phones in the area

In 2010, the FBI was looking for a pair of bank robbers known as the "high country bandits." Security footage from the banks wasn't very revealing, so the Bureau turned to cell phone companies for help. To find out who was consistently near the banks when these robberies took place, they asked for the number of every single phone that was connected to cell towers near the robbed banks around the time the crimes occurred. In response, they got back over 150,000 numbers. This is a cell tower dump: the practice of demanding an enormous amount of cell phone location information—anywhere from hundreds to hundreds of thousands of data points—in an effort to identify just a few suspects.

https://www.aclu.org/news/national-security/cell-tower-dumps-another-surveillance-technique

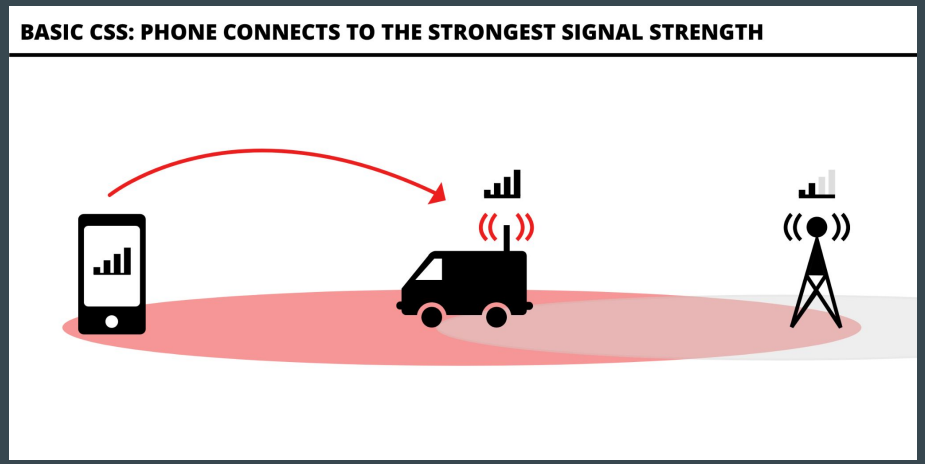
Celltower Dump



Phone network monitoring : IMSI Catchers

- Portable fake Base Station

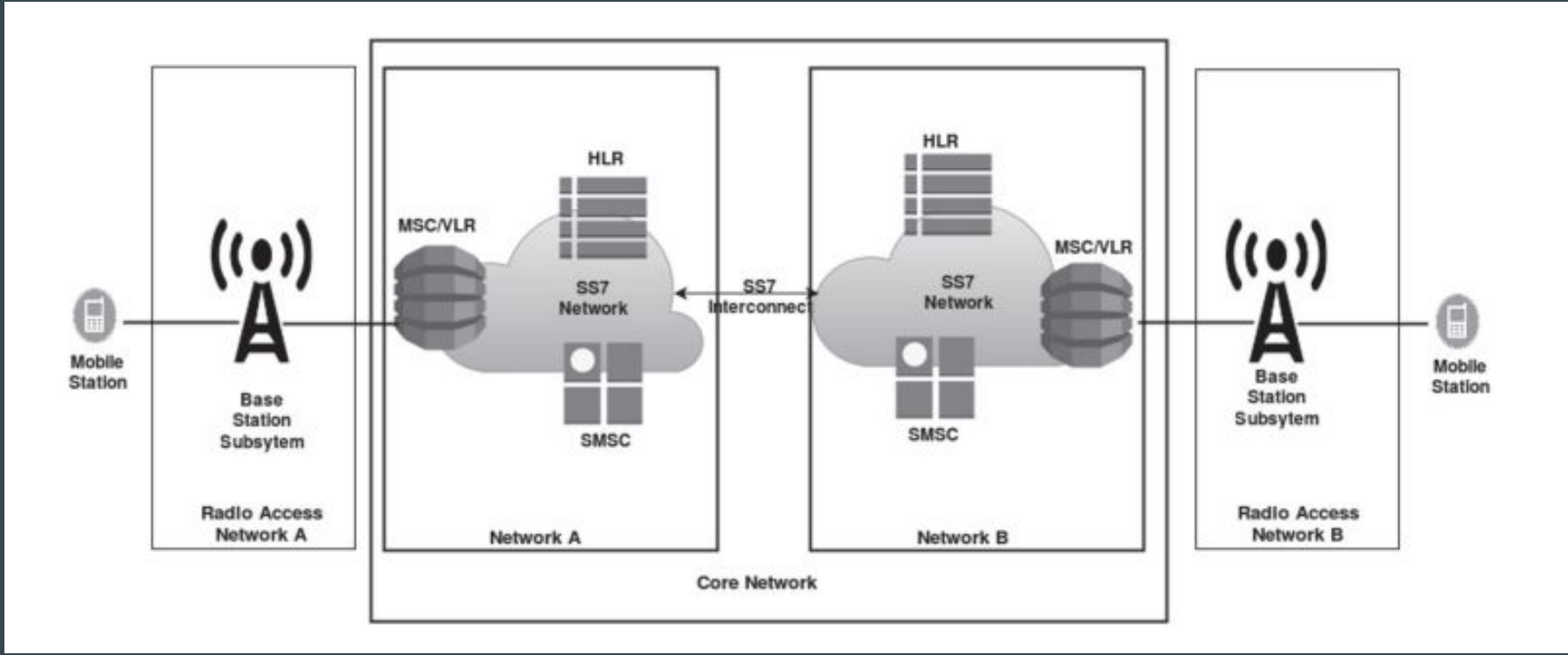
- Allows to identify IMSI numbers in the zone + potentially hijack phone and network traffic



https://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/
https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks

Phone network monitoring : IMSI Catchers

Phone network monitoring : SS7



Phone network monitoring : SS7

16.12.20 STATE SCRUTINY › BIG TECH

SPY COMPANIES USING CHANNEL ISLANDS TO TRACK PHONES AROUND THE WORLD

Private intelligence companies are using phone networks based in the Channel Islands to enable surveillance operations to be carried out against people around the world, including British and US citizens, the Bureau of Investigative Journalism can reveal following a joint reporting project with the Guardian.

Leaked data, documents and interviews with industry insiders who have access to sensitive information suggest that systemic weaknesses in the global telecoms infrastructure, and a particular vulnerability in Jersey and Guernsey, are being exploited by corporate spy businesses.

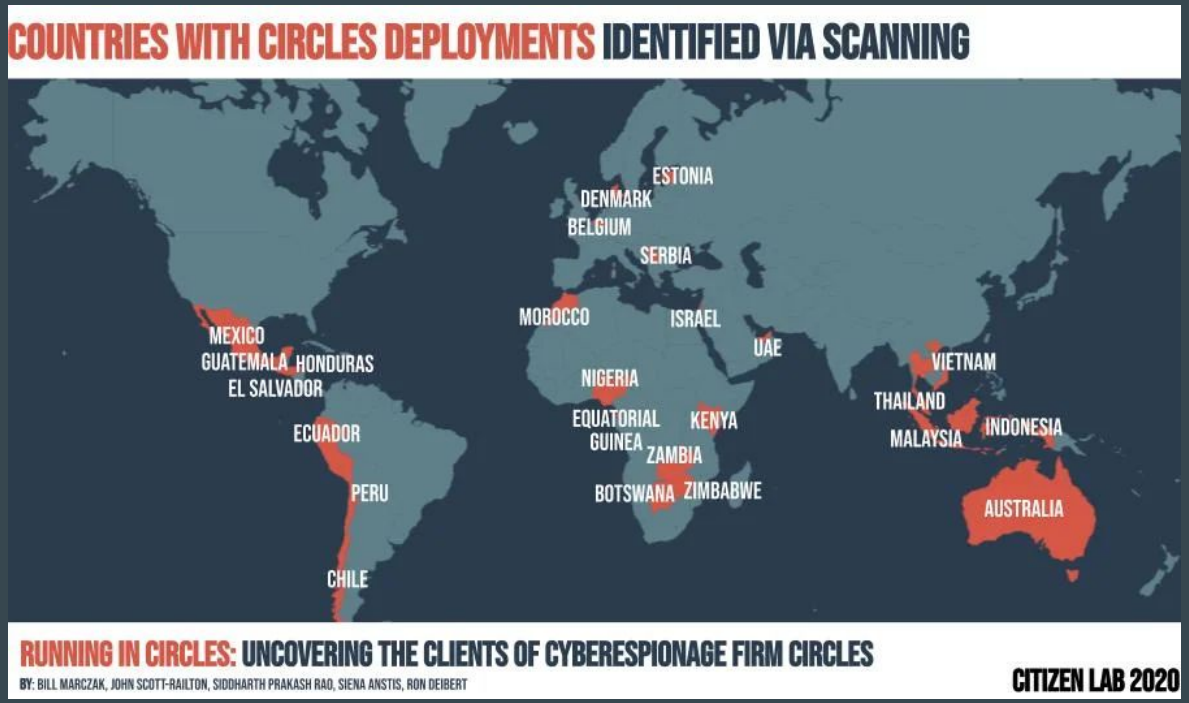
In one example, disclosed here for the first time, networks in the Channel Islands were used in an effort to locate Princess Latifa al-Maktoum as she attempted to evade her father, Sheikh Mohammed, the ruler of Dubai.

Latifa, who claimed that her father had her held in solitary confinement, in the dark, beaten and sedated over a period of several years when she was in her teens and early twenties (allegations which have been denied), fled the United Arab Emirates on a chartered yacht, but was recaptured off the coast of India a week later.

The yacht used in Princess Latifa's escape attempt

https://www.thebureauinvestigates.com/stories/2020-12-16/spy-companies-using-channel-islands-to-track-phones-around-the-world

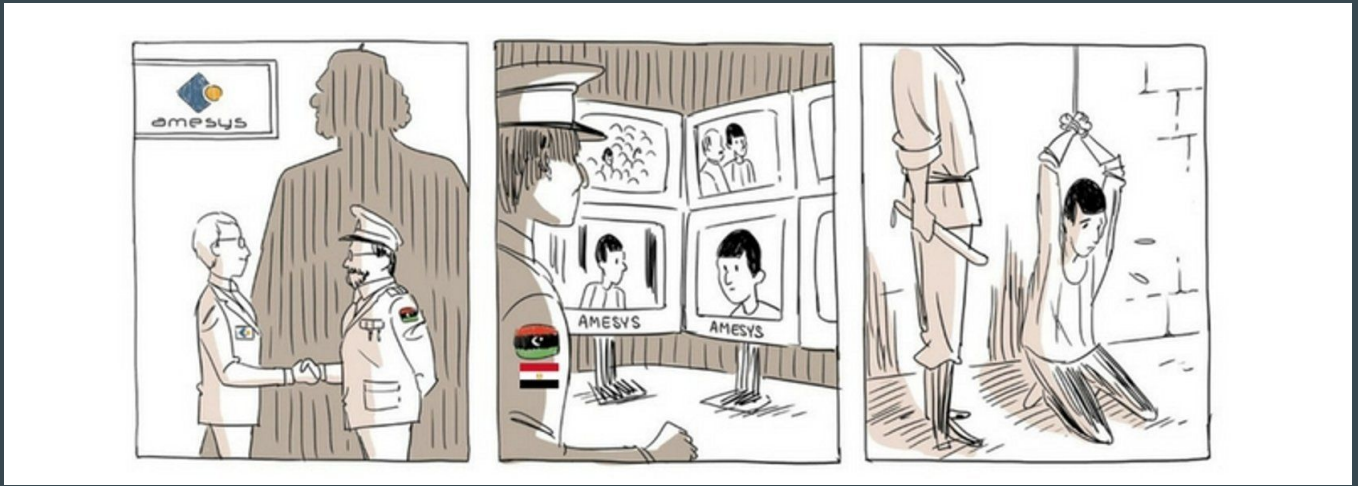
Phone network monitoring : SS7



https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

Internet Monitoring

- Many countries have installed systems to inspect internet traffic
- Deep Packet Inspection (or DPI)
- Most famous cases are the usage of French surveillance technology in Libya and Egypt

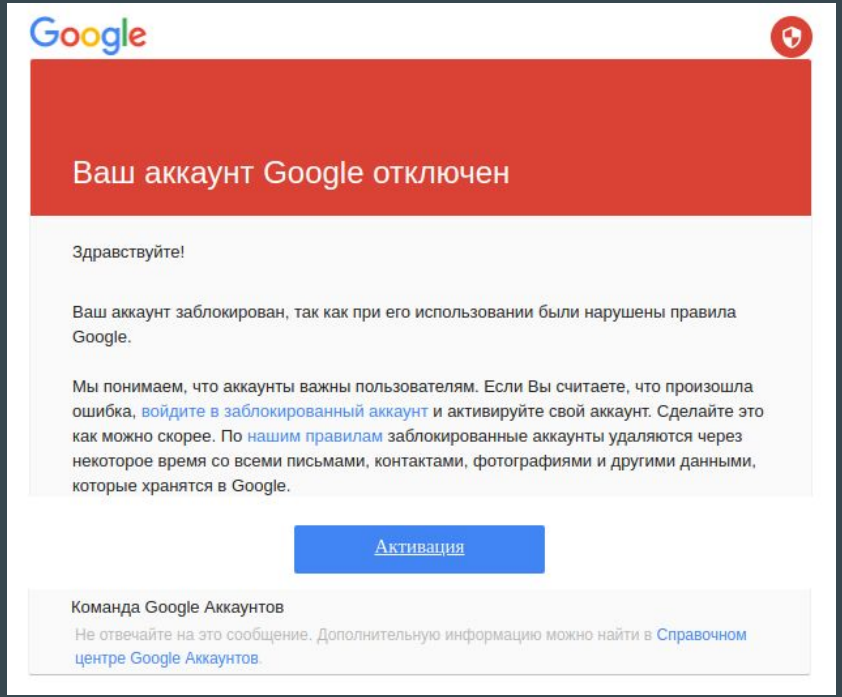


https://www.fidh.org/en/region/north-africa-middle-east/egypt/surveillance-and-torture-in-egypt-and-libya-amesys-and-nexa

Questions?
Break time!

Phishing

- Phishing campaigns are the most common threat
- It’s simple, yet it works
- Never underestimate attacks without technical complexity (even if they don’t make headlines)



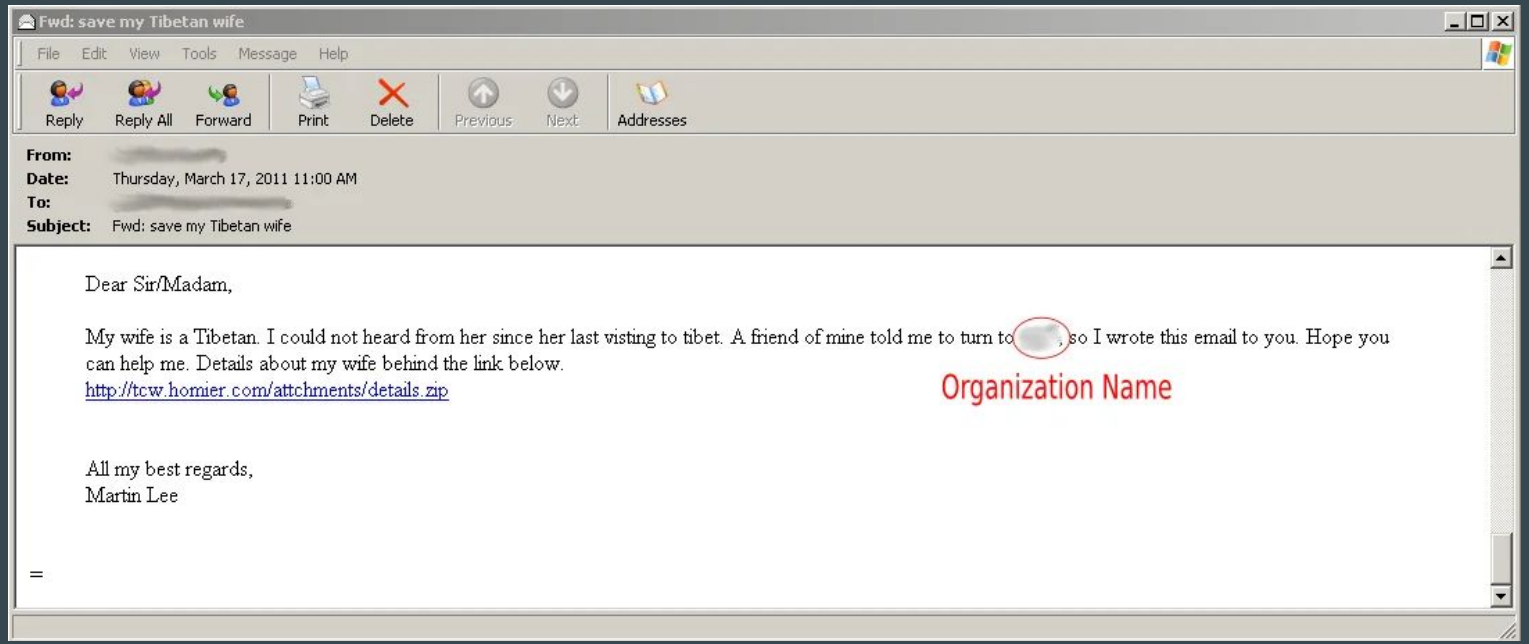
Phishing

> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [redacted]ta@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [redacted]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.

Ref:
https://www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/

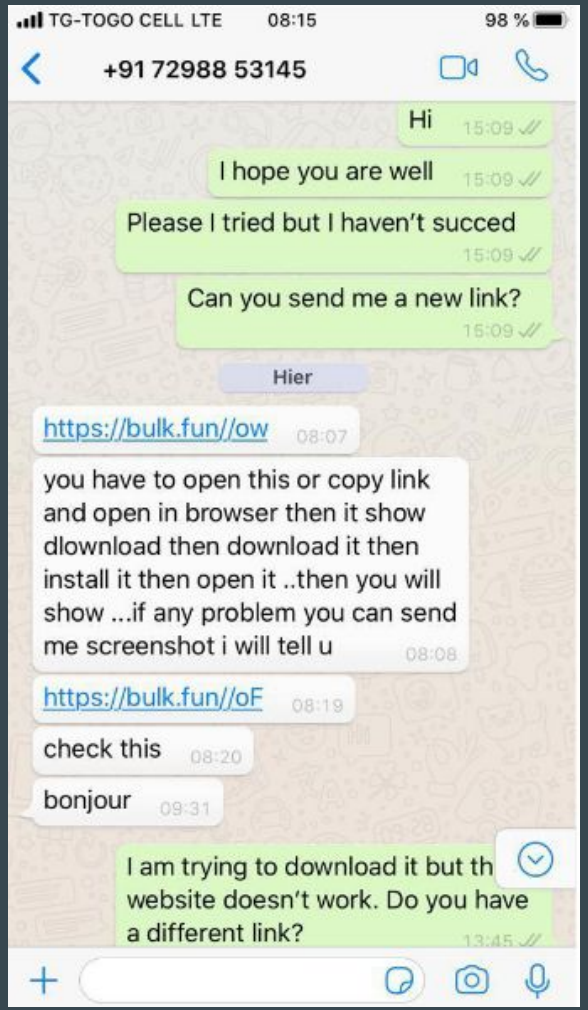
Spyware Attacks

In the same way, most spyware attacks are technically quite simple : attached files, files shared in a chat group



https://citizenlab.ca/2013/02/apt1s-glasses-watching-a-human-rights-organization/

Spyware Attacks



Ref:
https://www.amnesty.org/en/wp-content/uploads/2021/10/AFR5747562021ENGLISH.pdf

Advanced Spyware Attacks

https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

Amnesty International Among Targets of NSO-powered Campaign

Summary

In June 2018, an Amnesty International staff member received a malicious WhatsApp message with Saudi Arabia-related bait content and carrying links Amnesty International believes are used to distribute and deploy sophisticated mobile spyware. Through the course of our subsequent investigation we discovered that a Saudi activist based abroad had also received similar malicious messages. In its analysis of these messages, Amnesty International found connections with a network of over 600 domain names. Not only are these domain names suspicious, but they also overlap with infrastructure that had previously been identified as part of Pegasus, a sophisticated commercial exploitation and spyware platform sold by the Israel surveillance vendor, NSO Group.

Malicious Messages sent to Activists working on Human Rights in Saudi Arabia

In early June, an Amnesty International staff member received a suspicious message on their personal mobile device. The message, delivered through the WhatsApp messenger, carried a malicious link which Amnesty International believes belongs to infrastructure connected with NSO Group and previously documented attacks (see below for more information on these connections).

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

First 0 click Attacks

Privacy

WhatsApp blames — and sues — mobile spyware maker NSO Group over its zero-day calling exploit

Zack Whittaker @zackwhittaker / 8:21 PM GMT+1 • October 29, 2019

NSO Group in Morocco

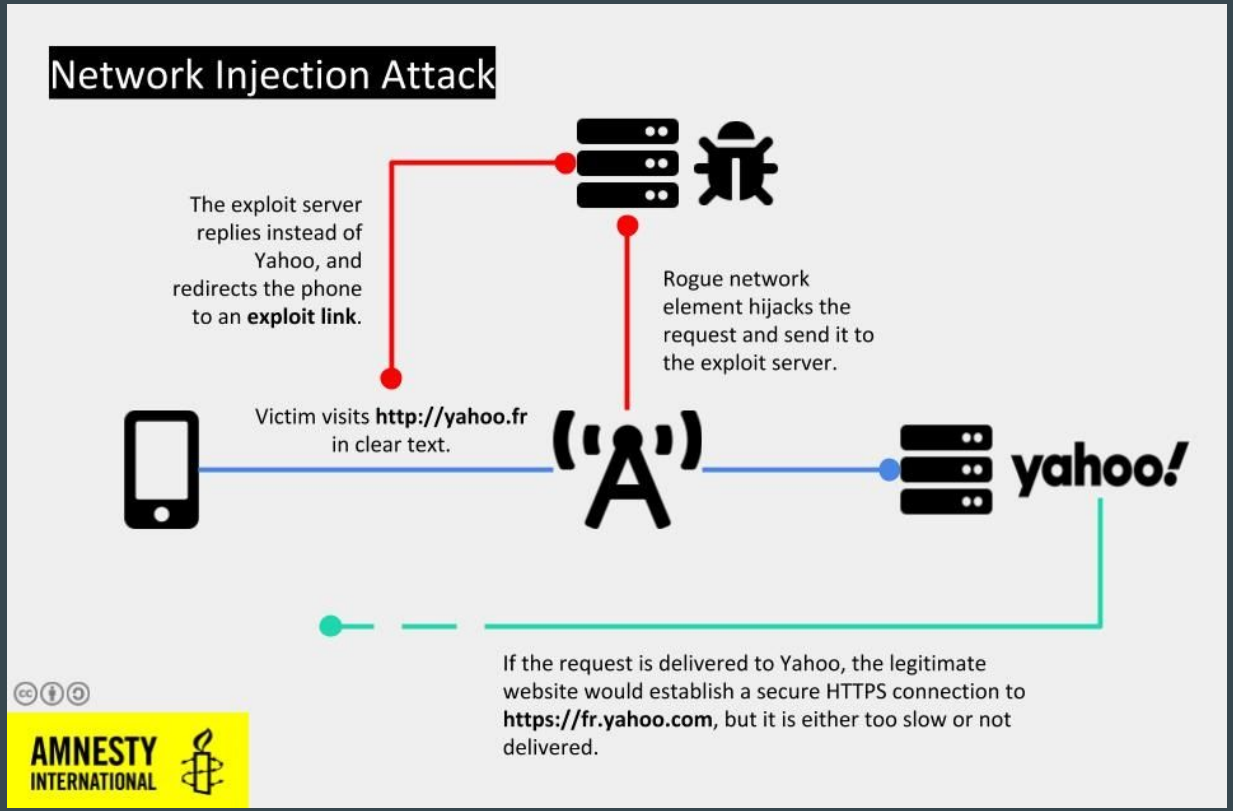
Maati Monjib
Human Rights Defender

		Translation
2 Nov 2017 at 12:29	Truecaller à le plaisir de vous annoncer l'ajout d'une nouvelle functionnalité, consulter le noms des personnes qui ont cherché votre numéro durant une semaine http://tinyurl.com/redacted	Truecaller has the pleasure to announce the addition of a new functionality, check the name of the people who searched your number in the last week. [exploit link]
15 Nov 2017 at 17:05	فضيحة أخلاقية داخل مقهى بورتز في حي أكدال بالرباطلمشاهدة الفيديو الذي يوثق الفضيحةhttps://videosdownload.co/redacted	A moral scandal inside Portz Café in the Agdal district in Rabat. To see the video documenting the scandal. [exploit link]
7 Dec 2017 at 18:21	ALQODS RESTERA TOUJOURS LA CAPITALE DE LA PALESTINE SAUVEZ LA VILLE SAINTE EN SIGNANT CETTE PETITION http://tinyurl.com/redacted	Jerusalem will remain the capital of Palestine Save the holy city by signing this petition. [exploit link]
8 Jan 2018 at 12:58	Urgent le livre sur Donald Trump s est arrache dans toutes les libraires une version arabe est disponible gratuitement sur le lien http://tinyurl.com/redacted	Urgent the book on Donald Trump is selling fast in all book shops an arabic version is available for free at the following link. [exploit link]

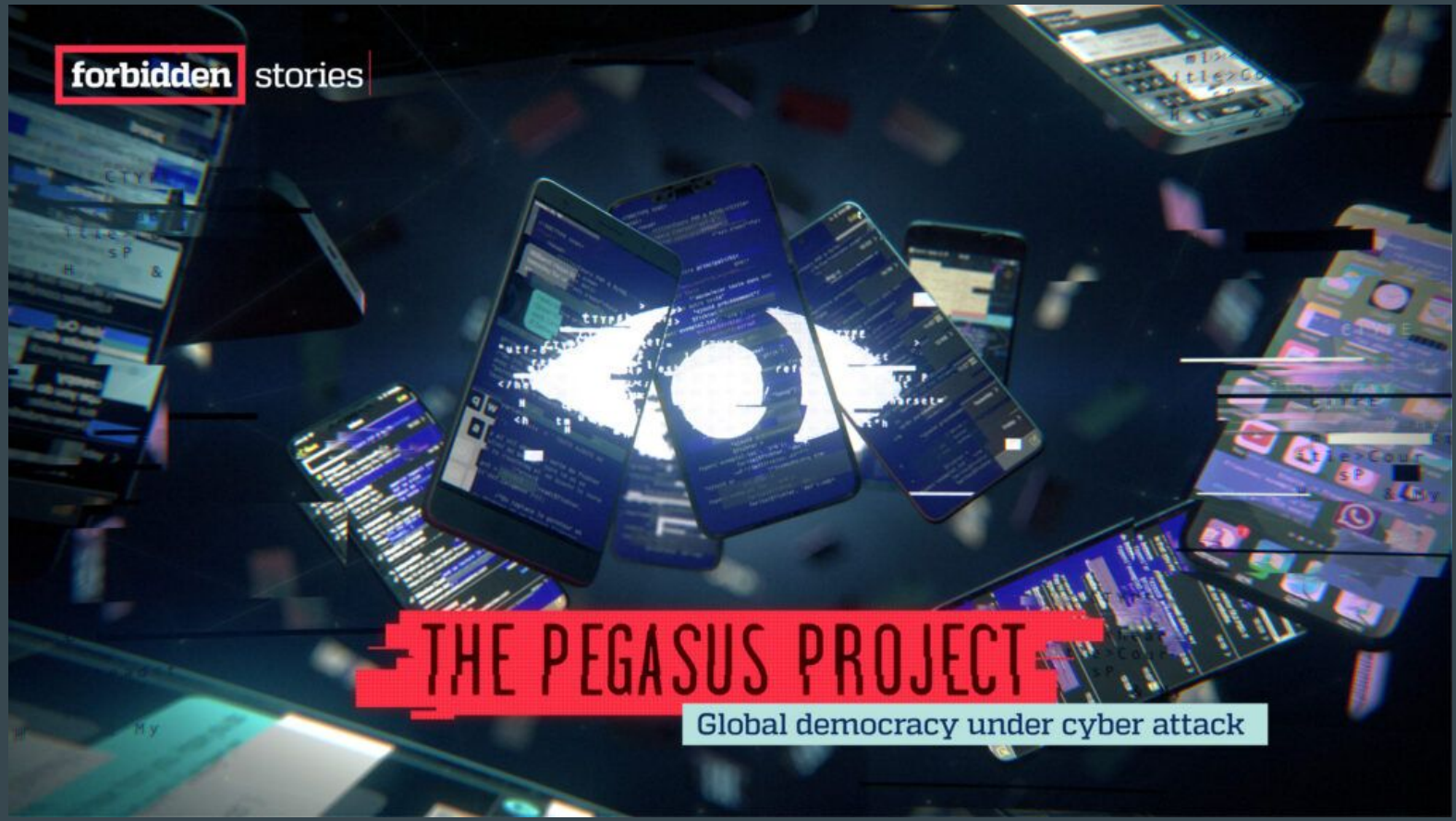
AMNESTY INTERNATIONAL

https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/

Network Traffic Injection



https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/



https://forbiddenstories.org/about-the-pegasus-project/

Lessons Learnt from Pegasus Project

- Spyware abuse isn’t only a Middle East Issue
- Most attacks were using 0 click attacks abusing Apple apps on iPhones
- Exploitation was often done for just a few days to optimize licences

APT Groups

APT28

APT28 is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165.[1][2] This group has been active since at least 2004.[3][4][5][6][7][8][9][10][11][12][13]

APT28 reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. [5] In 2018, the US indicted five GRU Unit 26165 officers associated with APT28 for cyber operations (including close-access operations) conducted between 2014 and 2018 against the World Anti-Doping Agency (WADA), the US Anti-Doping Agency, a US nuclear facility, the Organization for the Prohibition of Chemical Weapons (OPCW), the Spiez Swiss Chemicals Laboratory, and other organizations.[14] Some of these were conducted with the assistance of GRU Unit 74455, which is also referred to as Sandworm Team.

GROUPS

Overview
admin@338
Ajax Security Team
ALLANITE
Andariel
Aoqin Dragon
APT-C-36
APT1
APT12
APT16
APT17
APT18
APT19
APT28
APT29
APT3
APT30

Home > Groups

Groups

Groups are activity clusters that are tracked by a common name in the security community. Analysts track these clusters using various analytic methodologies and terms such as threat groups, activity groups, and threat actors. Some groups have multiple names associated with similar activities due to various organizations tracking similar activities by different names. Organizations' group definitions may partially overlap with groups designated by other organizations and may disagree on specific activity.

For the purposes of the Group pages, the MITRE ATT&CK team uses the term Group to refer to any of the above designations for an adversary activity cluster. The team makes a best effort to track overlaps between names based on publicly reported associations, which are designated as "Associated Groups" on each page (formerly labeled "Aliases"), because we believe these overlaps are useful for analyst awareness. We do not represent these names as exact overlaps and encourage analysts to do additional research.

Groups are mapped to publicly reported technique use and original references are included. The information provided does not represent all possible technique use by Groups, but rather a subset that is available solely through open source reporting. Groups are also mapped to reported Software used and attributed Campaigns, and related techniques for each are tracked separately on their respective pages.

Groups: 135

ID	Name	Associated Groups	Description
G0018	admin@338		admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as PoisonIvy, as well as some non-public backdoors.
G0130	Ajax Security Team	Operation Woolen-Goldfish, AjaxTM, Rocket Kitten, Flying Kitten, Operation Saffron Rose	Ajax Security Team is a group that has been active since at least 2010 and believed to be operating out of Iran. By 2014 Ajax Security Team transitioned from website defacement operations to malware-based cyber espionage campaigns targeting the US defense industrial base and Iranian users of anti-censorship technologies.

https://attack.mitre.org/

The Spyware Industry

Candiru

Quadream

Hacker for hire

Exclusive: Obscure Indian cyber firm spied on politicians, investors worldwide

By Jack Stubbs, Raphael Satter, Christopher Bing

7 MIN READ

(This June 9 story corrects to remove reference to speaking with Gupta at his office)

BellTroX

A Customer Driven Company

"you desire, we do!"

Forensics Tools

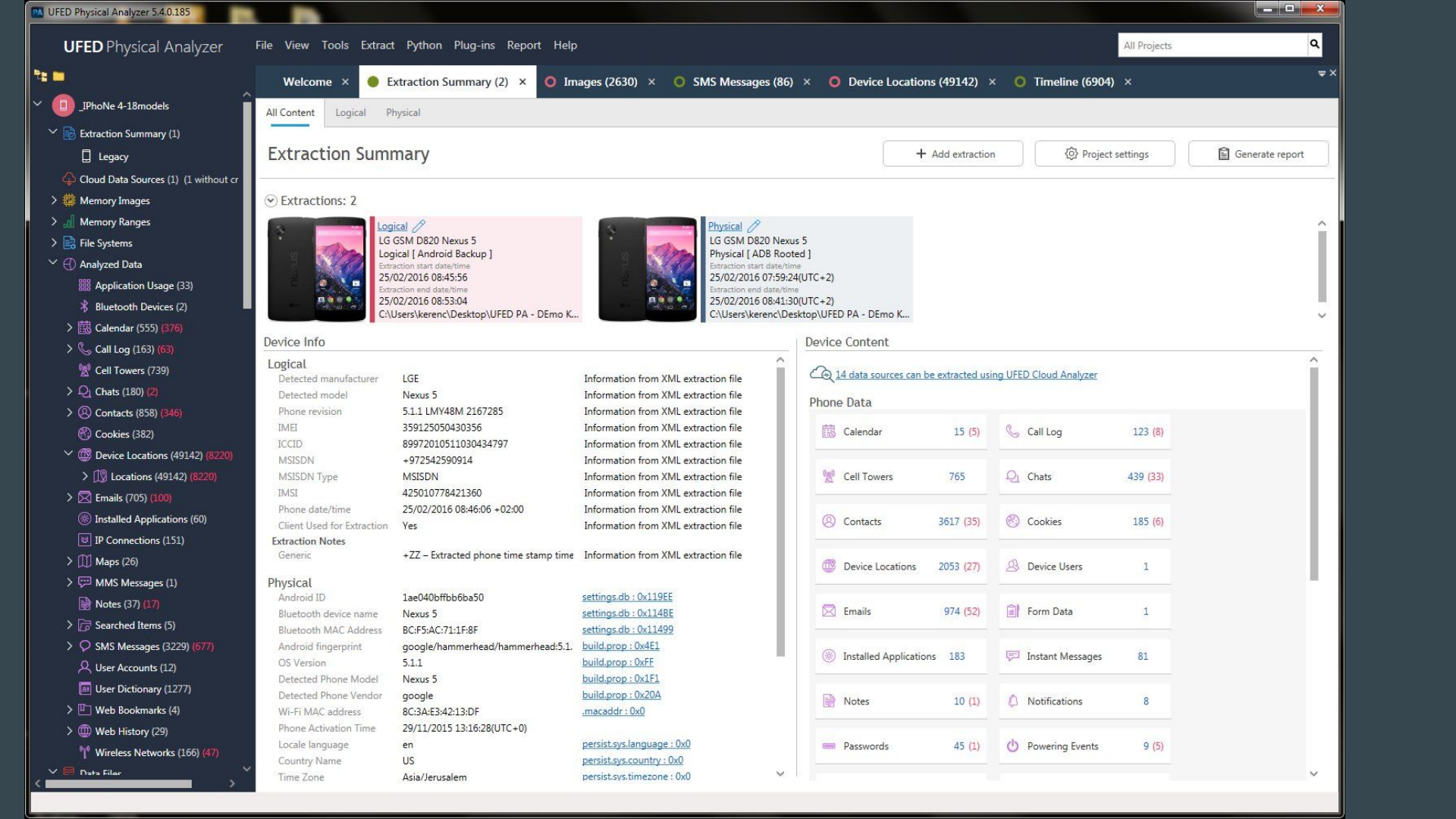
- Owned by most police forces in the world
- The leading company is Cellebrite, but also GrayKey, Magnet Forensics

Haaretz | Israel News

Israeli Phone-hacking Firm Cellebrite Halts Sales to Russia, Belarus in Wake of Haaretz Report

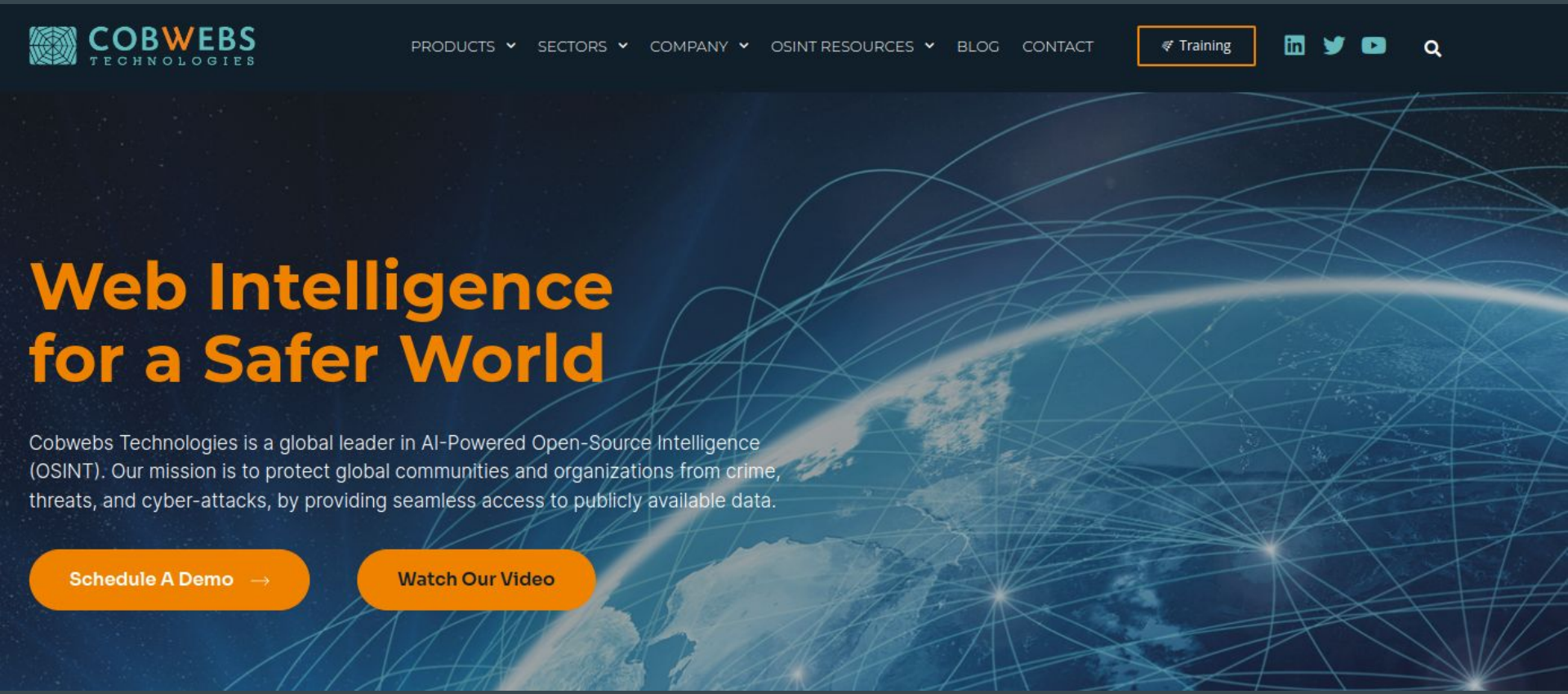
Cellebrite will stop selling hacking tools to Russia and Belarus after its technology was used against minorities, pro-democracy activists and opposition forces

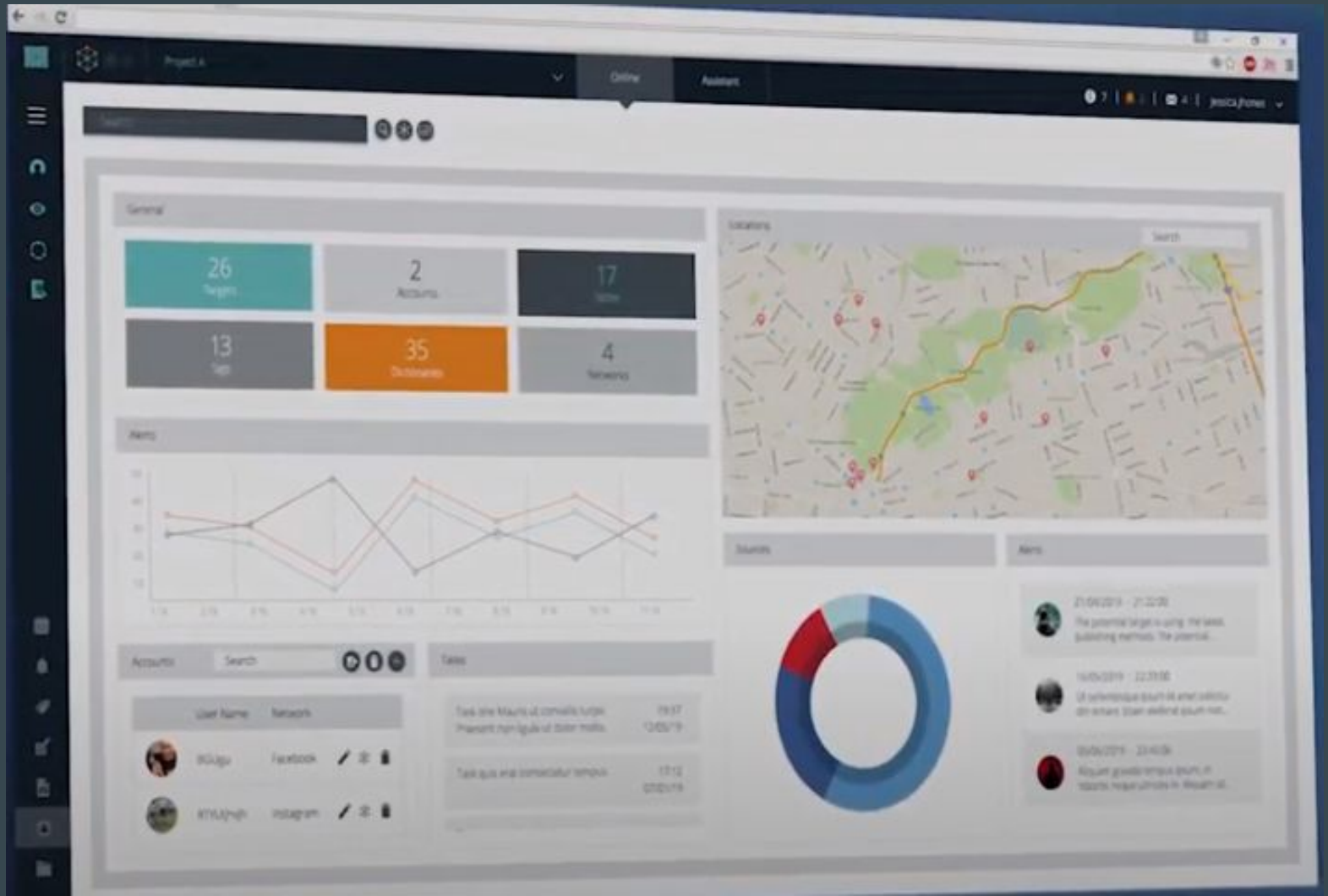
https://www.haaretz.com/israel-news/2021-03-18/ty-article/.premium/israeli-phone-hacking-firm-cellebrite-halts-sales-to-russia-after-haaretz-report/0000017f-ef02-d8a1-a5ff-ff8a33350000

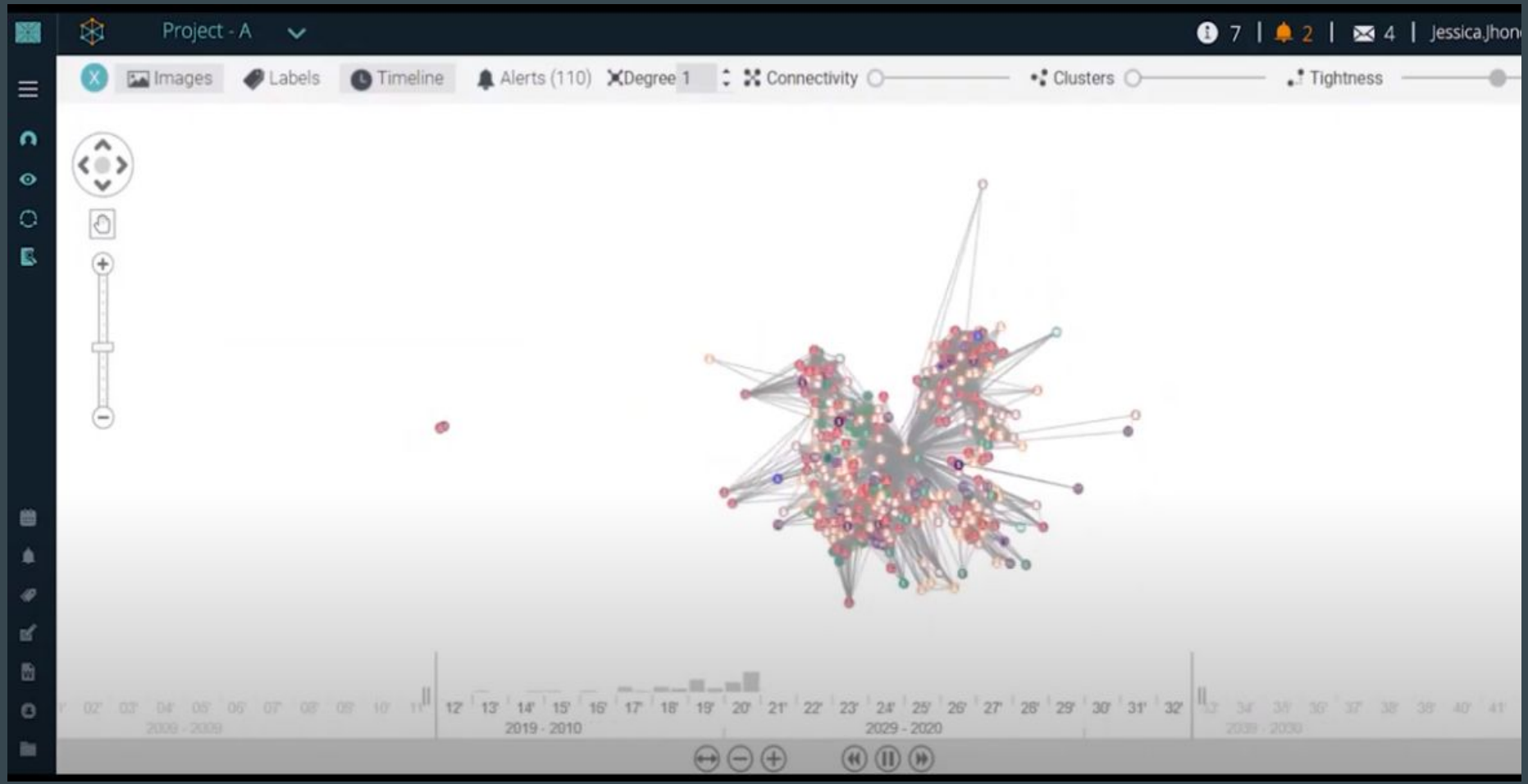

UFED Physical Analyzer 5.4.0.185
UFED Physical Analyzer
File View Tools Extract Python Plug-ins Report Help
All Projects
Welcome
Extraction Summary (2)
Images (2630)
SMS Messages (86)
Device Locations (49142)
Timeline (6904)
All Content
Logical
Physical
Extraction Summary
Add extraction
Project settings
Generate report
Extractions: 2
Logical
LG GSM D820 Nexus 5
Logical [Android Backup]
Extraction start date/time
25/02/2016 08:45:56
Extraction end date/time
25/02/2016 08:53:04
C:\Users\kerenc\Desktop\UFED PA - DEmo K...
Physical
LG GSM D820 Nexus 5
Physical [ADB Rooted]
Extraction start date/time
25/02/2016 07:59:24(UTC+2)
Extraction end date/time
25/02/2016 08:41:30(UTC+2)
C:\Users\kerenc\Desktop\UFED PA - DEmo K...
Device Info
Logical
Detected manufacturer LGE Information from XML extraction file
Detected model Nexus 5 Information from XML extraction file
Phone revision 5.1.1 LMY48M 2167285 Information from XML extraction file
IMEI 359125050430356 Information from XML extraction file
ICCID 89972010511030434797 Information from XML extraction file
MSISDN +972542590914 Information from XML extraction file
MSISDN Type MSISDN Information from XML extraction file
IMSI 425010778421360 Information from XML extraction file
Phone date/time 25/02/2016 08:46:06 +02:00 Information from XML extraction file
Client Used for Extraction Yes Information from XML extraction file
Extraction Notes
Generic +ZZ – Extracted phone time stamp time Information from XML extraction file
Physical
Android ID 1ae040bffbb6ba50 settings.db : 0x119EE
Bluetooth device name Nexus 5 settings.db : 0x114BE
Bluetooth MAC Address BC:F5:AC:71:1F:8F settings.db : 0x11499
Android fingerprint google/hammerhead/hammerhead:5.1. build.prop : 0x4E1
OS Version 5.1.1 build.prop : 0xFF
Detected Phone Model Nexus 5 build.prop : 0x1F1
Detected Phone Vendor google build.prop : 0x20A
Wi-Fi MAC address 8C:3A:E3:42:13:DF .macaddr : 0x0
Phone Activation Time 29/11/2015 13:16:28(UTC+0)
Locale language en persist.sys.language : 0x0
Country Name US persist.sys.country : 0x0
Time Zone Asia/Jerusalem persist.sys.timezone : 0x0
Device Content
14 data sources can be extracted using UFED Cloud Analyzer
Phone Data
Calendar 15 (5)
Call Log 123 (8)
Cell Towers 765
Chats 439 (33)
Contacts 3617 (35)
Cookies 185 (6)
Device Locations 2053 (27)
Device Users 1
Emails 974 (52)
Form Data 1
Installed Applications 183
Instant Messages 81
Notes 10 (1)
Notifications 8
Passwords 45 (1)
Powering Events 9 (5)
_IPhoNe 4-18models
Extraction Summary (1)
Legacy
Cloud Data Sources (1) (1 without cr
Memory Images
Memory Ranges
File Systems
Analyzed Data
Application Usage (33)
Bluetooth Devices (2)
Calendar (555) (376)
Call Log (163) (63)
Cell Towers (739)
Chats (180) (2)
Contacts (858) (346)
Cookies (382)
Device Locations (49142) (8220)
Locations (49142) (8220)
Emails (705) (100)
Installed Applications (60)
IP Connections (151)
Maps (26)
MMS Messages (1)
Notes (37) (17)
Searched Items (5)
SMS Messages (3229) (677)
User Accounts (12)
User Dictionary (1277)
Web Bookmarks (4)
Web History (29)
Wireless Networks (166) (47)

WEBINT / OSINT

- Platforms gathering open source information from social networks, internet etc.
- Hard to know what is true and what is BS
- In reality probably combining this data with many other sources


COBWEBS
TECHNOLOGIES
PRODUCTS
SECTORS
COMPANY
OSINT RESOURCES
BLOG
CONTACT
Training
Web Intelligence
for a Safer World
Cobwebs Technologies is a global leader in AI-Powered Open-Source Intelligence (OSINT). Our mission is to protect global communities and organizations from crime, threats, and cyber-attacks, by providing seamless access to publicly available data.
Schedule A Demo →
Watch Our Video


26
2
17
13
35
4


Project - A
7
2
4
Jessica.Jhon
Images
Labels
Timeline
Alerts (110)
Degree 1
Connectivity
Clusters
Tightness
2019 - 2010
2029 - 2020

WEBINT / OSINT

SCRAPING

As a common tactic used as part of the *Reconnaissance phase* (and to later enable *Engagement* and *Exploitation*), we've observed companies that sell these capabilities (and their clients) using fake accounts and software tools to scrape information from social media and other public websites. This first stage of the surveillance chain is typically the least visible to the targets, who are silently profiled by spyware entities on behalf of their clients.

Firms selling these capabilities often market themselves as "web intelligence services" to enable collection, retention, analysis and searchability. In addition to obfuscating the ultimate beneficiaries of spyware services, they also significantly lower the barrier of entry for their customers.

They typically use fake accounts to search and view people's profiles and other publicly available information. They can be managed by the service provider for its clients, or operated by the customers themselves through software provided by the surveillance-for-hire firm.

We removed a number of these firms, including a New York-based company called Social Links, an Israel-based company called Cyber Globes, a Russia-based firm called Avalanche and an unattributed entity in China.

https://about.fb.com/wp-content/uploads/2022/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf

WEBINT / OSINT

SCRAPING

As a common tactic used as part of the *Reconnaissance phase* (and to later enable *Engagement* and *Exploitation*), we've observed companies that sell these capabilities (and their clients) using fake accounts and software tools to scrape information from social media and other public websites. This first stage of the surveillance chain is typically the least visible to the targets, who are silently profiled by spyware entities on behalf of their clients.

Firms selling these capabilities often market themselves as "web intelligence services" to enable collecti
beneficiaries o
customers.

They typically
information. Th
customers the

We removed a
an Israel-based
unattributed e

OOO Lavina Puls (Lavina Puls) and **AO Inforus** (Inforus) have provided technical support to malign influence operations conducted by the GRU, including the management of false social media personas. The Kremlin has used these tools of malign covert influence to attack democracy in the United States, Ukraine, and around the world. **Andrey Igorevich Masalovich** (Masalovich), the head of Lavina Puls and Inforus, has worked to sell the internet monitoring and influence technology he designed for the GRU internationally. The United States and its allies will continue to take action to ensure that those who seek to export the Russian government's brand of authoritarianism cannot do so with impunity. Lavina Puls, Inforus, and Masalovich were designated pursuant to E.O. 14024 for operating or having operated in the technology sector of the Russian Federation economy.

CYBERSECURITY • DAILY COVER

Exclusive: Meet Russia's Cambridge Analytica, Run By A Former KGB Agent Turned YouTube Influencer

https://www.forbes.com/sites/thomasbrewster/2023/03/21/andrei-masalovich-avalanche-russia-cambridge-analytica/

ADINT

- ADvertisement INTelligence
- Trackers in everyday apps, gathering geolocation of millions of people and reselling it for intelligence

MOTHERBOARD
TECH BY VICE

How the U.S. Military Buys Location Data from Ordinary Apps

A Muslim prayer app with over 98 million downloads is one of the apps connected to a wide-ranging supply chain that sends ordinary people's personal data to brokers, contractors, and the military.

By Joseph Cox

https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x

ADINT

DELL CAMERON SECURITY MAR 8, 2023 2:45 PM

The FBI Just Admitted It Bought US Location Data

Rather than obtaining a warrant, the bureau purchased sensitive data—a controversial practice that privacy advocates say is deeply problematic.

https://www.wired.com/story/fbi-purchase-location-data-wray-senate/

ADINT

From an OSINT vendor brochure : “This gives rise to the idea of ADINT or Ad-Intelligence. ADINT aims to use global mobile advertising data to achieve unique intelligence insights without deploying any special sensor equipment.

The most powerful application of ADINT is to perform a massive geolocation. Our DEEP ADINT platform collects data from multiple mobile ad platforms such as XXX and XXX.

By using multiple sources and multiple ad formats, our platform is able to achieve high coverage of users in a particular geographic area. The platform allows the compilation of various types of location-based data sources, for use as search, analysis, and monitoring of an individual or area. The information is displayed in a simple interface and uses an interactive display map. Interactive maps allow users to filter and analyze intelligence data facilitating investigations.”

Bonus : Disinformation

Venezuela and the United States

We removed 24 Facebook accounts, 54 Pages and four accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated in Venezuela and the United States and targeted Guatemala and Honduras.

We found this activity after receiving a tip from journalists at Reuters. Although the people behind the operation attempted to conceal their identities and coordination, our investigation found links to Predictvia, a Florida-registered firm, operating from both Venezuela and the United States. We banned this company from our services and issued a Cease and Desist letter.

often reposted other people's content with long-form commentary, in addition to sharing original posts by the operation's fictitious media brands. Some of these accounts had Cyrillic names and were likely acquired from account farms in Eastern Europe, and some Pages displayed Twitter handles in their cover images on Facebook.

The individuals behind this effort shared memes and long- and short-form text posts in Spanish. They ran two targeted efforts focused on mayoral politics in Guatemala and national politics in Honduras. In Guatemala, this network focused on criticizing the current mayor of San Juan Sacatepéquez. In Honduras, they focused on political corruption and criticism of the president of the Honduran Congress, while posting supportive commentary about the Liberal Party.

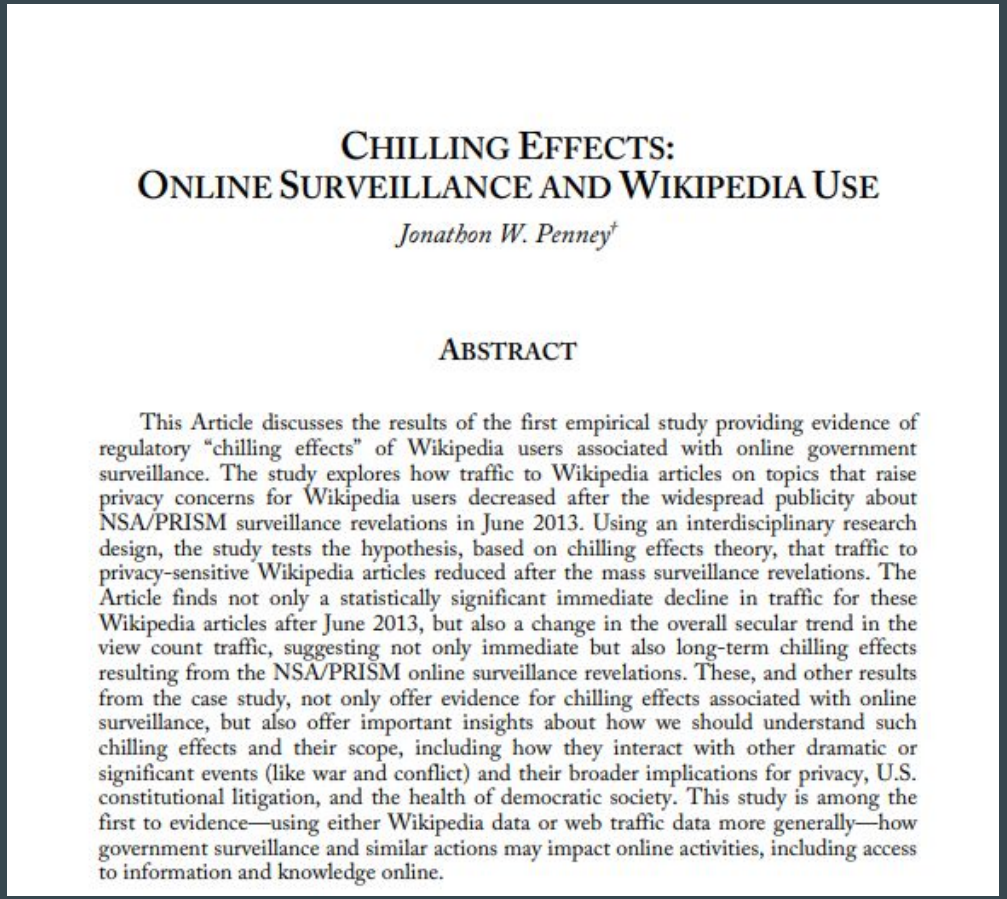
https://about.fb.com/wp-content/uploads/2023/05/Meta-Quarterly-Adversarial-Threat-Report-Q1-2023.pdf

Questions?
Break time!

Impact of Digital Surveillance

Chilling Effect

Feeling surveilled clearly has an effect on freedom of expression



CHILLING EFFECTS: ONLINE SURVEILLANCE AND WIKIPEDIA USE

Jonathon W. Penney[†]

ABSTRACT

This Article discusses the results of the first empirical study providing evidence of regulatory "chilling effects" of Wikipedia users associated with online government surveillance. The study explores how traffic to Wikipedia articles on topics that raise privacy concerns for Wikipedia users decreased after the widespread publicity about NSA/PRISM surveillance revelations in June 2013. Using an interdisciplinary research design, the study tests the hypothesis, based on chilling effects theory, that traffic to privacy-sensitive Wikipedia articles reduced after the mass surveillance revelations. The Article finds not only a statistically significant immediate decline in traffic for these Wikipedia articles after June 2013, but also a change in the overall secular trend in the view count traffic, suggesting not only immediate but also long-term chilling effects resulting from the NSA/PRISM online surveillance revelations. These, and other results from the case study, not only offer evidence for chilling effects associated with online surveillance, but also offer important insights about how we should understand such chilling effects and their scope, including how they interact with other dramatic or significant events (like war and conflict) and their broader implications for privacy, U.S. constitutional litigation, and the health of democratic society. This study is among the first to evidence—using either Wikipedia data or web traffic data more generally—how government surveillance and similar actions may impact online activities, including access to information and knowledge online.

Psychological Impact

- Under-researched topic
- Clearly, being hacked has an important psychological impact on some people
- As journalists, think about it when investigating digital surveillance

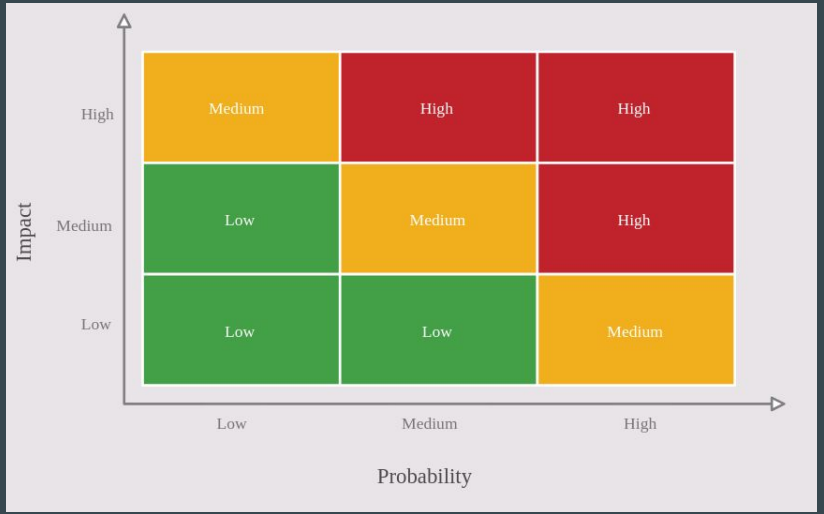
Digital Security

Rule n°1: yes, you can improve your digital security

Digital Security : need for methods & tools

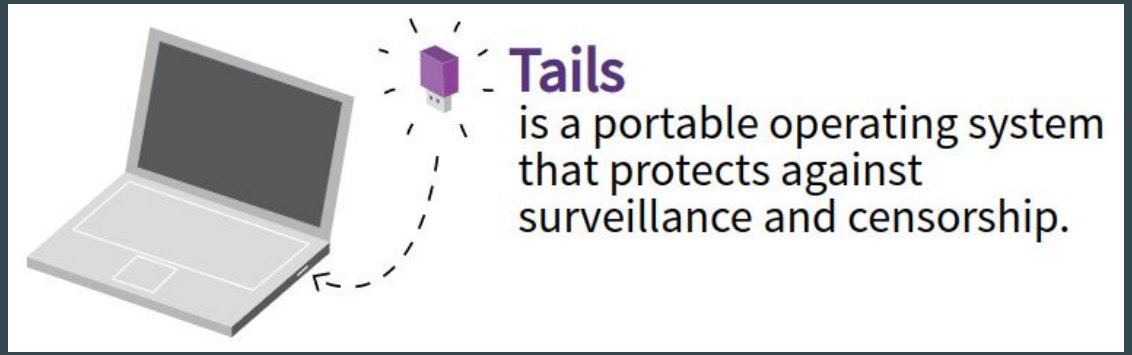
Method 1 : Assess the threats you are facing

- In the physical world, we do threat analysis all the time
- It doesn't work in an innate way online, we need to do a conscious threat analysis
- It's pretty simple :
  - List the digital threats you may face, all of them
  - Estimate the probability and impact
  - Each time a risk is too high, find solutions against it



Method 2 : Compartmentalize

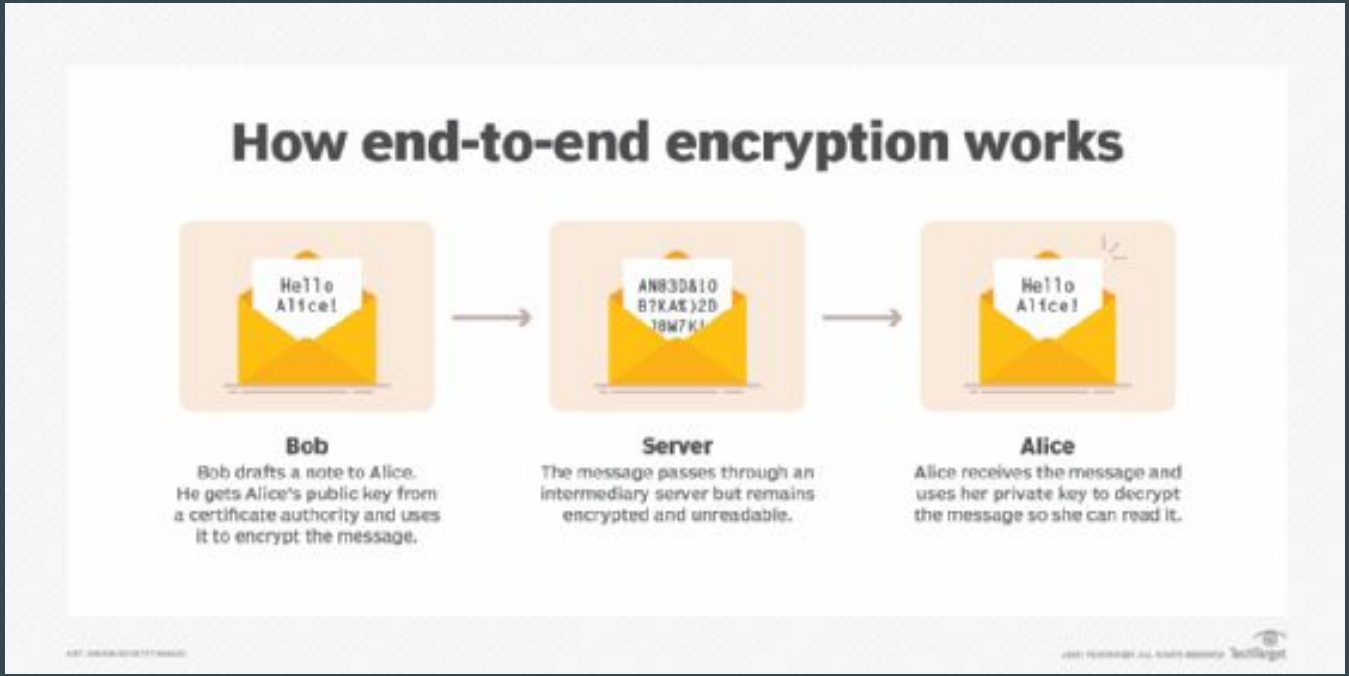
- Sometimes you can’t afford to fail
- Compartmentalize everything!
- Tails help, but a different hardened phone with new phone number can work



Method 3 : Understand digital security and know when to get support

- You will need to have some solid bases at digital security
- AND know when you don’t know and need to ask support
- Find tech people you trust and work with them

Tools 1 : End to end encryption FTW

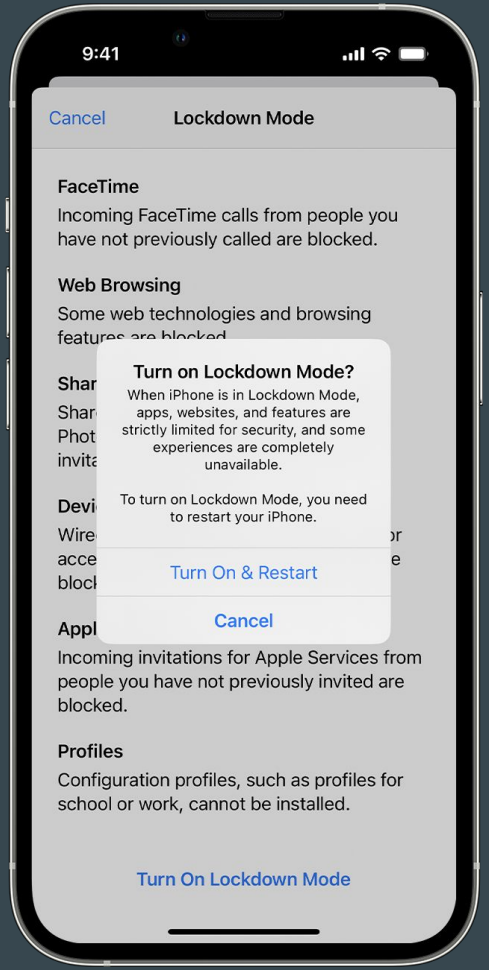


Tools 1 : End to end encryption FTW

- Unbelievable 10 years ago, now easily available in many places
- / ! \ with metadata !
- Now everywhere in chat apps
- But also available in some web apps
- Bonus : use disappearing messages

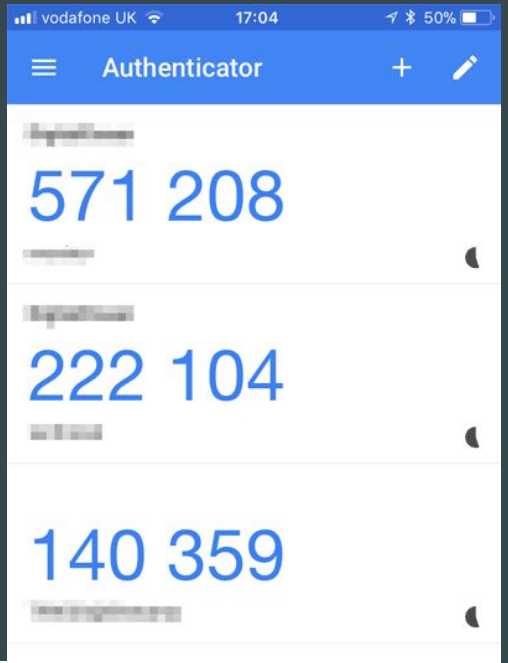
Tools 2 : Secure Your Phone

- Securing devices is a complex process
- Major improvements in smartphone security over the past years
- iPhones : keep it up to date + Lockdown mode
- Android :
    - Harder, the most secure is probably a Pixel with latest updates
    - If you want extra security, try Graphene OS



Tools 3 : Use Two Factor Authentication

- Key aspect to improve security of your online accounts
- Second factor beside your password
- Any 2FA is better than 2FA, but
  - Try to avoid SMS
  - If you can, use hardware keys



Ressources


SURVEILLANCE
SELF-DEFENSE


security in-a-box
digital security tools and tactics


accessnow

Questions?

Bonus discussion : working with tech experts

- Be clear on what you are looking for
- Develop trust relationship
- Double check their technical analysis still

For Thursday

Pick one of the investigations from the use-cases and read it in depth. Dig into the details : how is this surveillance working? How was the investigation done? Can you learn more about this type of surveillance?

We will talk about each case on Thursday.