Cosa gli altri possono fare con nostri i dati e metadati

Gabriele Zanoni

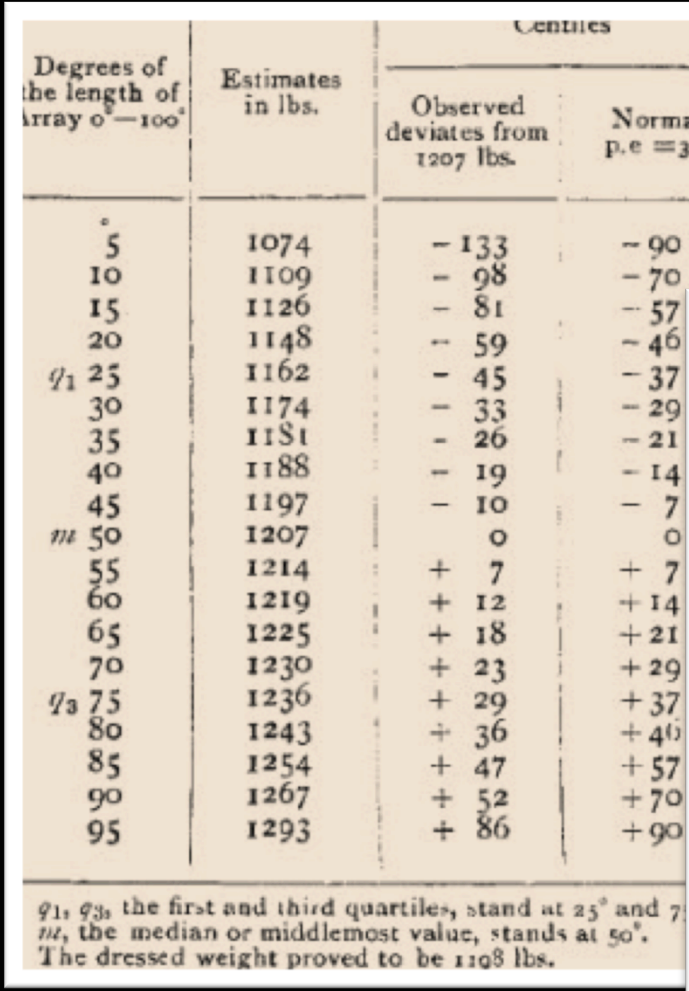
EMEA Incident Response Investigator
@infoshaker

Who's Who

- Cloud Security
- Penetration testing
- Incident Response
- Anti-Fraud
- Computer Forensics
- Mobile Security

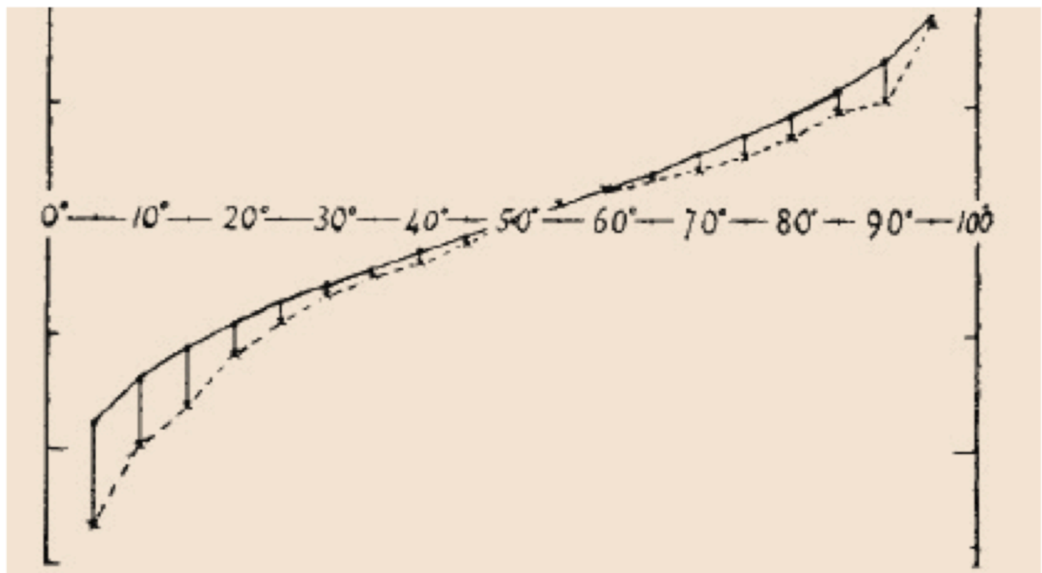
The power of analysis

Nobody knows…together we know!



Degrees of the length of Array 0°—100°	Estimates in lbs.	Centiles		Excess of Observed over Normal
		Observed deviates from 1207 lbs.	Normal p.e =37	
° 5	1074	−133	−90	+43
10	1109	− 98	−70	+28
15	1126	− 81	−57	
20	1148	− 59	−46	
q_1 25	1162	− 45	−37	
30	1174	− 33	−29	
35	1181	− 26	−21	
40	1188	− 19	−14	
45	1197	− 10	− 7	
m 50	1207	0	0	
55	1214	+ 7	+ 7	
60	1219	+ 12	+14	
65	1225	+ 18	+21	
70	1230	+ 23	+29	
q_3 75	1236	+ 29	+37	
80	1243	+ 36	+46	
85	1254	+ 47	+57	
90	1267	+ 52	+70	
95	1293	+ 86	+90	

q_1, q_3, the first and third quartiles, stand at 25° and 7
m, the median or middlemost value, stands at 50°.
The dressed weight proved to be 1198 lbs.



The continuous line is the normal curve with p.e.=37.
The broken line is drawn from the observations.
The lines connecting them show the differences between the observed and the normal.

- http://wisdomofcrowds.blogspot.it/2009/12/vox-populi-sir-francis-galton.html

Who is using OSINT ?

"For the past three years, Elaine Rich and 3,000 other average people have been quietly making probability estimates about everything from Venezuelan gas subsidies to North Korean politics as part of , an experiment put together by three well-known psychologists and some people inside the intelligence community."

"According to one report, the predictions made by the Good Judgment Project are often better even than intelligence analysts with access to classified information, and many of the people involved in the project have been astonished by its success at making accurate predictions."

- http://www.npr.org/blogs/parallels/2014/04/02/297839429/-so-you-think-youre-smarter-than-a-cia-agent
- http://www.goodjudgmentproject.com/

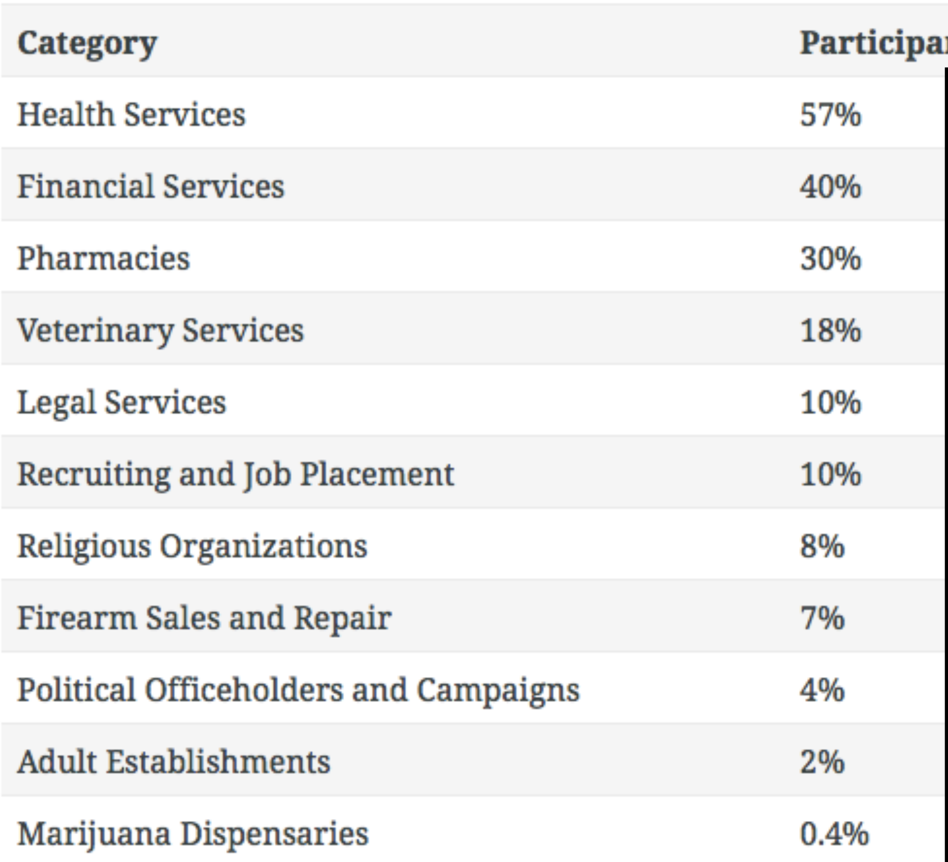
How our data and metadata could be used

Metadata analysis from phone calls 1/2

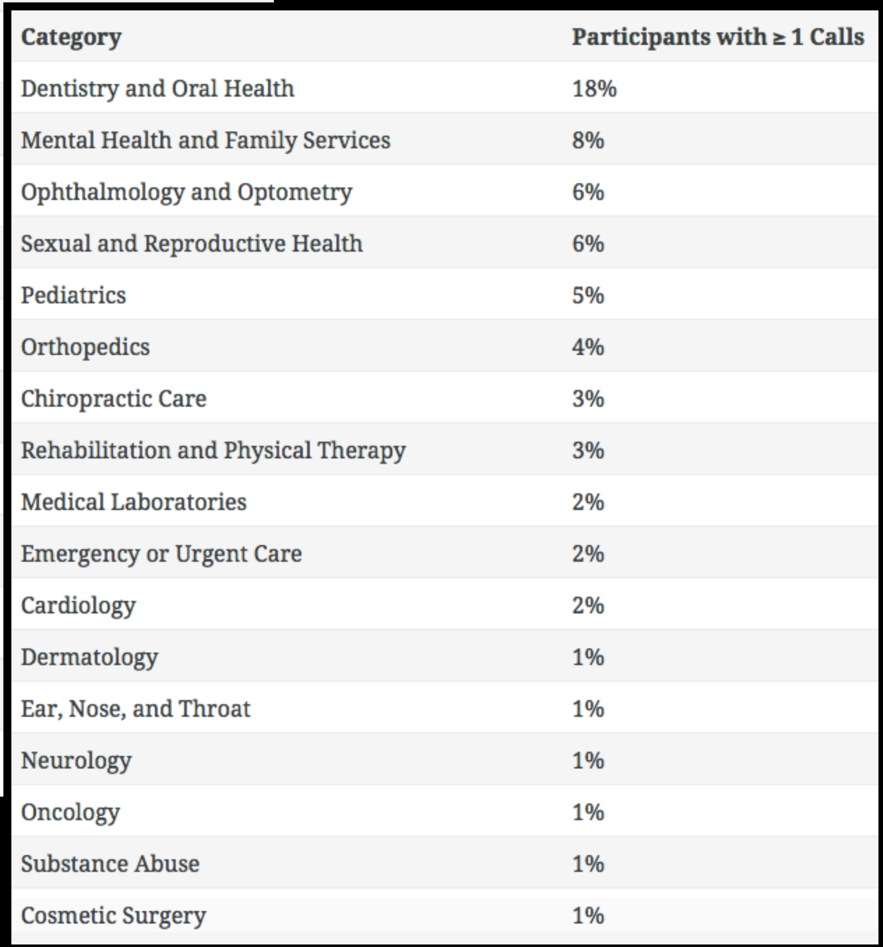
- An experiment from **Jonathan Mayer**
- "Participants run the MetaPhone app on their Android smartphone; it submits device logs and social network information for analysis."
- "We began by identifying the MetaPhone participants' contacts. We used the same approach as in our prior work on number identifiability, matching phone numbers against the public Yelp and Google Places directories. In total, our 546 participants contacted 33,688 unique numbers. 6,107 of those numbers (18%) resolved to an identity."

  – http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/

Metadata analysis from phone calls 2/2



Category	Participants with ≥ 1 Calls
Health Services	57%
Financial Services	40%
Pharmacies	30%
Veterinary Services	18%
Legal Services	10%
Recruiting and Job Placement	10%
Religious Organizations	8%
Firearm Sales and Repair	7%
Political Officeholders and Campaigns	4%
Adult Establishments	2%
Marijuana Dispensaries	0.4%



Category	Participants with ≥ 1 Calls
Dentistry and Oral Health	18%
Mental Health and Family Services	8%
Ophthalmology and Optometry	6%
Sexual and Reproductive Health	6%
Pediatrics	5%
Orthopedics	4%
Chiropractic Care	3%
Rehabilitation and Physical Therapy	3%
Medical Laboratories	2%
Emergency or Urgent Care	2%
Cardiology	2%
Dermatology	1%
Ear, Nose, and Throat	1%
Neurology	1%
Oncology	1%
Substance Abuse	1%
Cosmetic Surgery	1%

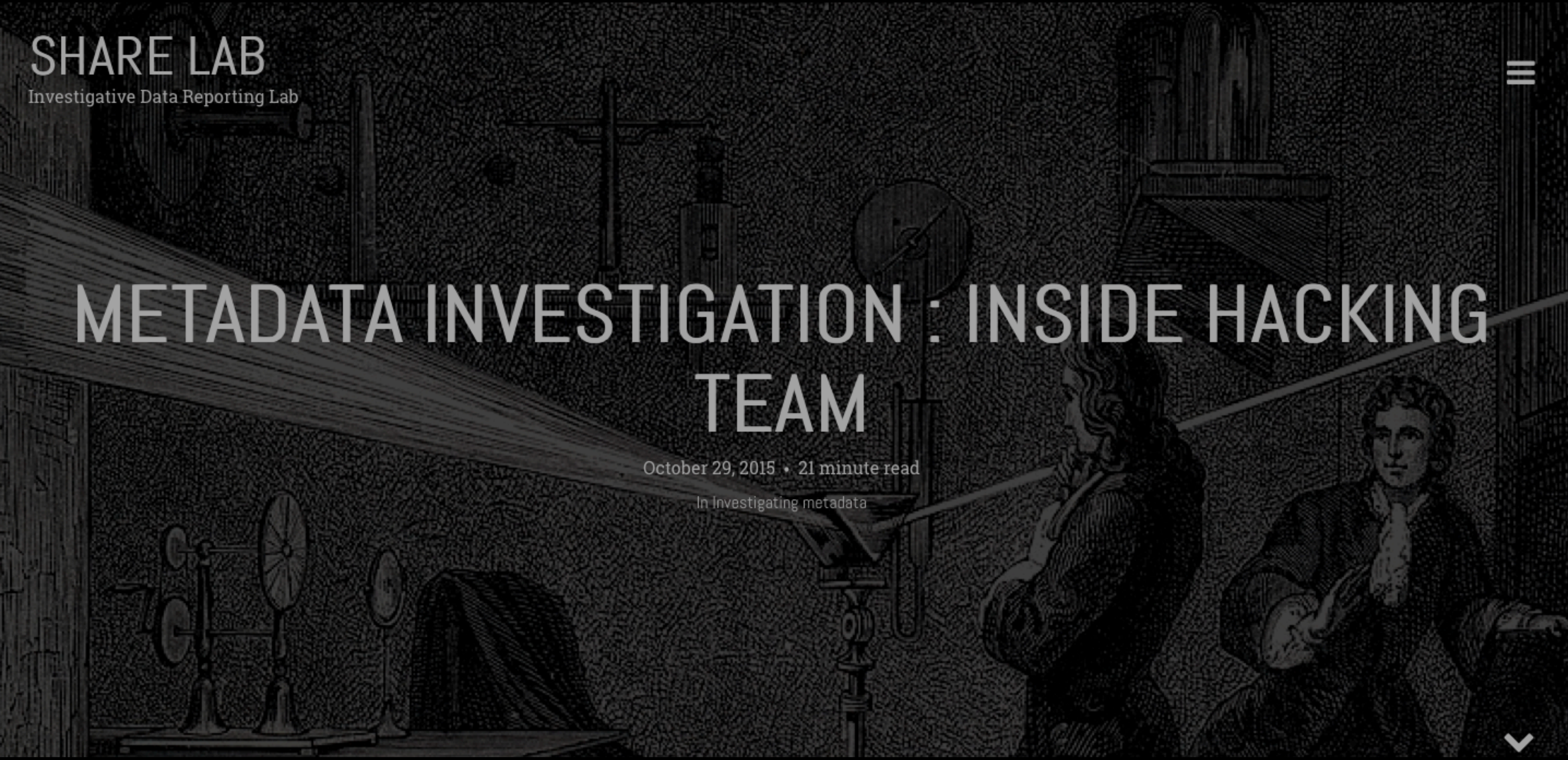
- http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/

Metadata analysis from phone calls: Pattern Results

- "A pattern of calls will often, of course, reveal more than individual call records. "
  - Participant A communicated with multiple local neurology groups, a specialty pharmacy, a rare condition management service, and a hotline for a pharmaceutical used solely to treat relapsing multiple sclerosis.
  - Participant B spoke at length with cardiologists at a major medical center, talked briefly with a medical laboratory, received calls from a pharmacy, and placed short calls to a home reporting hotline for a medical device used to monitor cardiac arrhythmia.
  - Participant C made a number of calls to a firearm store that specializes in the AR semiautomatic rifle platform. They also spoke at length with customer service for a firearm manufacturer that produces an AR line.
  - In a span of three weeks, Participant D contacted a home improvement store, locksmiths, a hydroponics dealer, and a head shop.
  - Participant E had a long, early morning call with her sister. Two days later, she placed a series of calls to the local Planned Parenthood location. She placed brief additional calls two weeks later, and made a final call a month after.

- http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/

https://labs.rs/en/metadata/



SHARE LAB

Investigative Data Reporting Lab

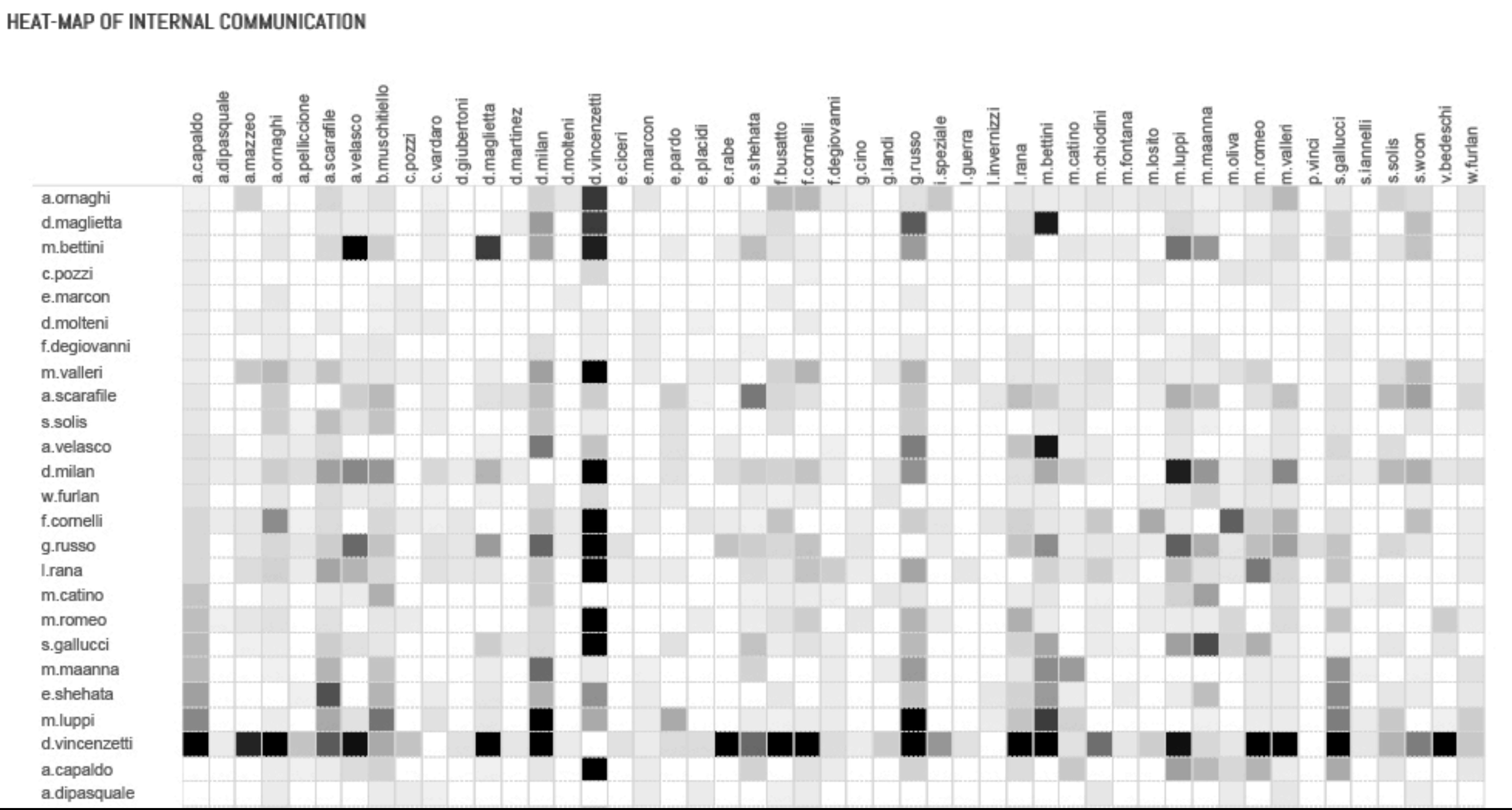
METADATA INVESTIGATION : INSIDE HACKING TEAM

October 29, 2015 • 21 minute read

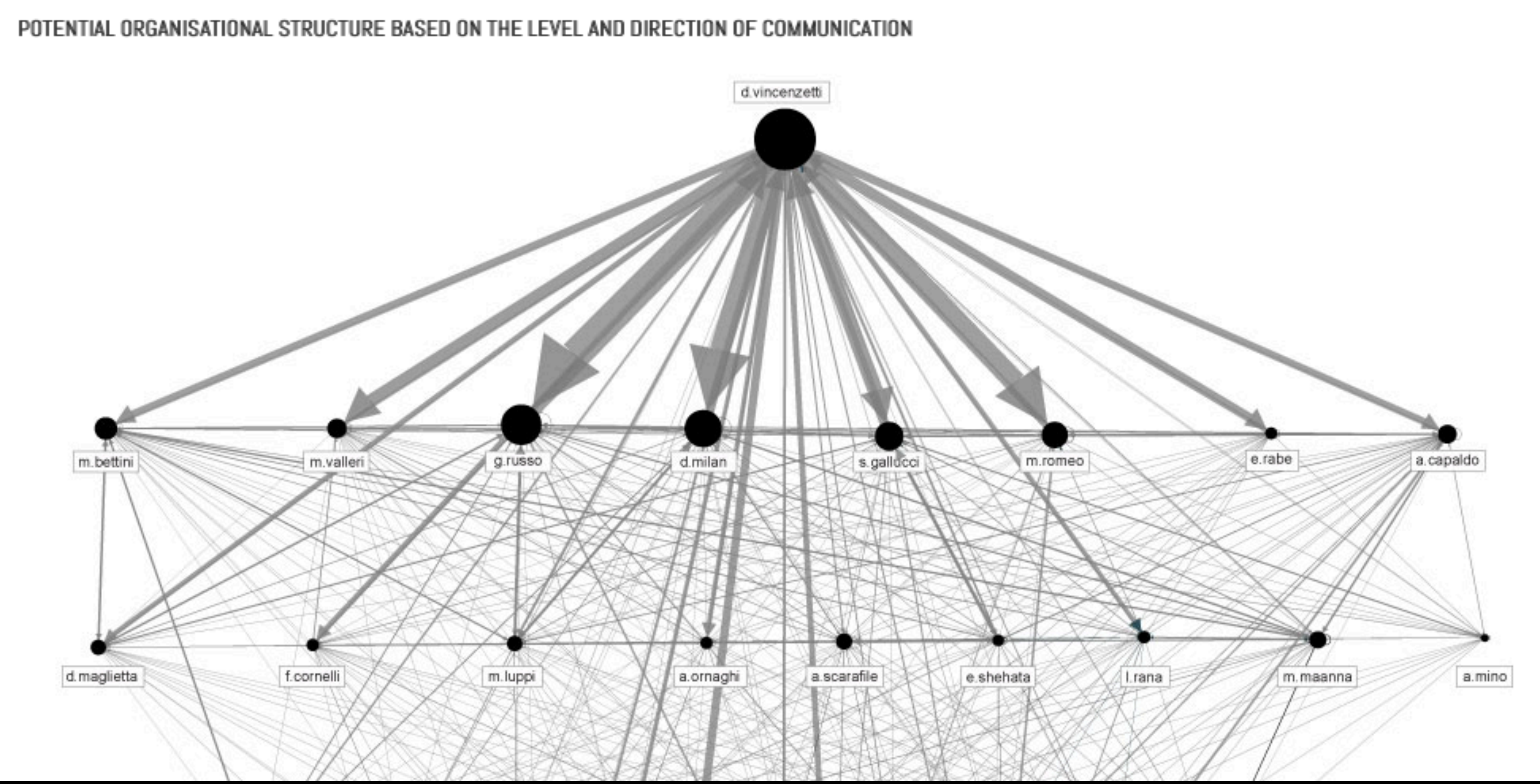
In investigating metadata

- Share Lab is a newborn child of the Share Foundation – a research and data investigation lab for exploring different technical aspects of the intersections between technology and society.
- “*Once online, our every movement, every click, sent or received email, our every activity produces a vast amount of invisible traces. These traces, once collected, put together and analysed, can reveal our behavioral patterns, location, contacts, habits and most intimate interests. They often reveal much more than we feel comfortable sharing.*”

- https://labs.rs/en/metadata/

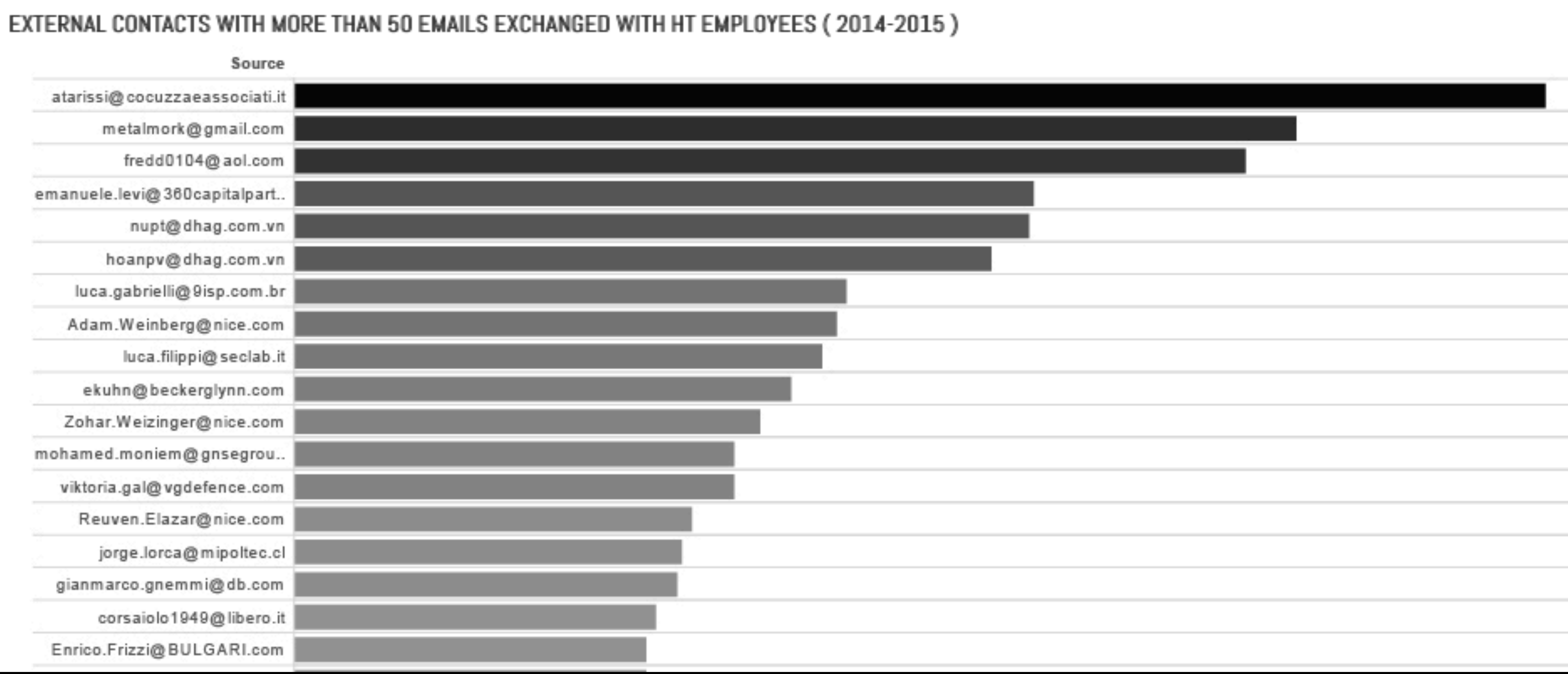


- https://labs.rs/en/metadata/

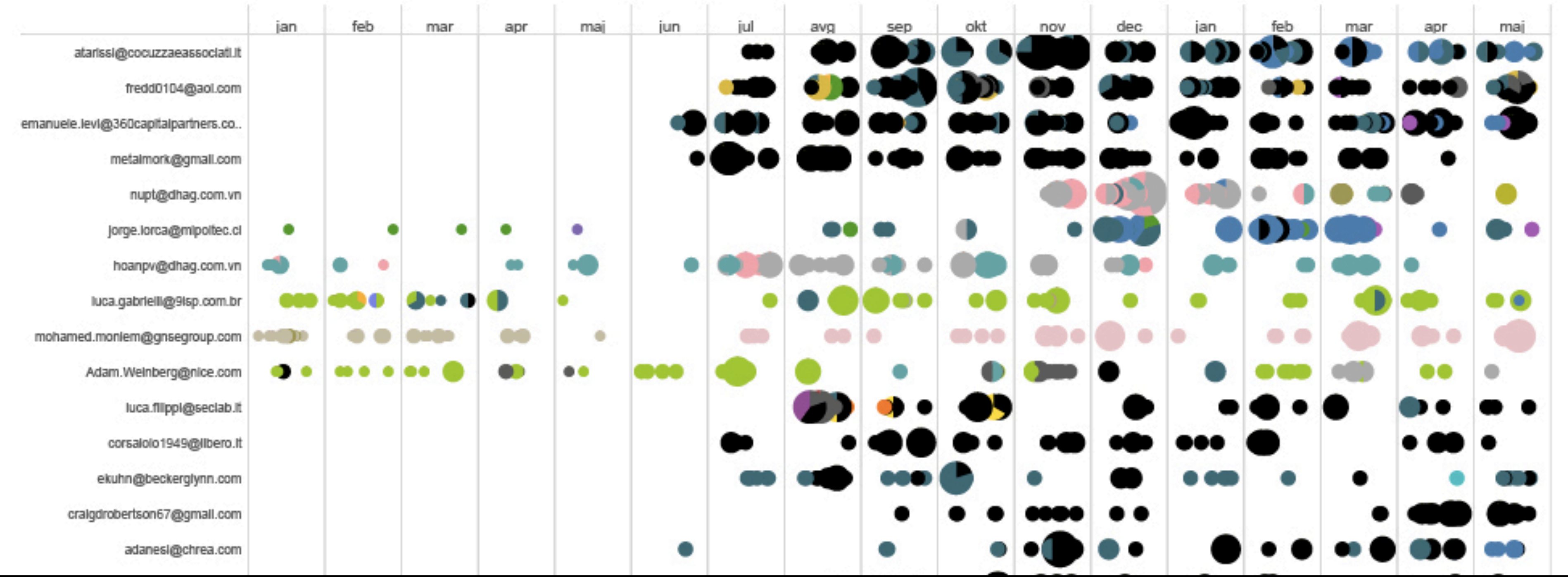


POTENTIAL ORGANISATIONAL STRUCTURE BASED ON THE LEVEL AND DIRECTION OF COMMUNICATION

- https://labs.rs/en/metadata/

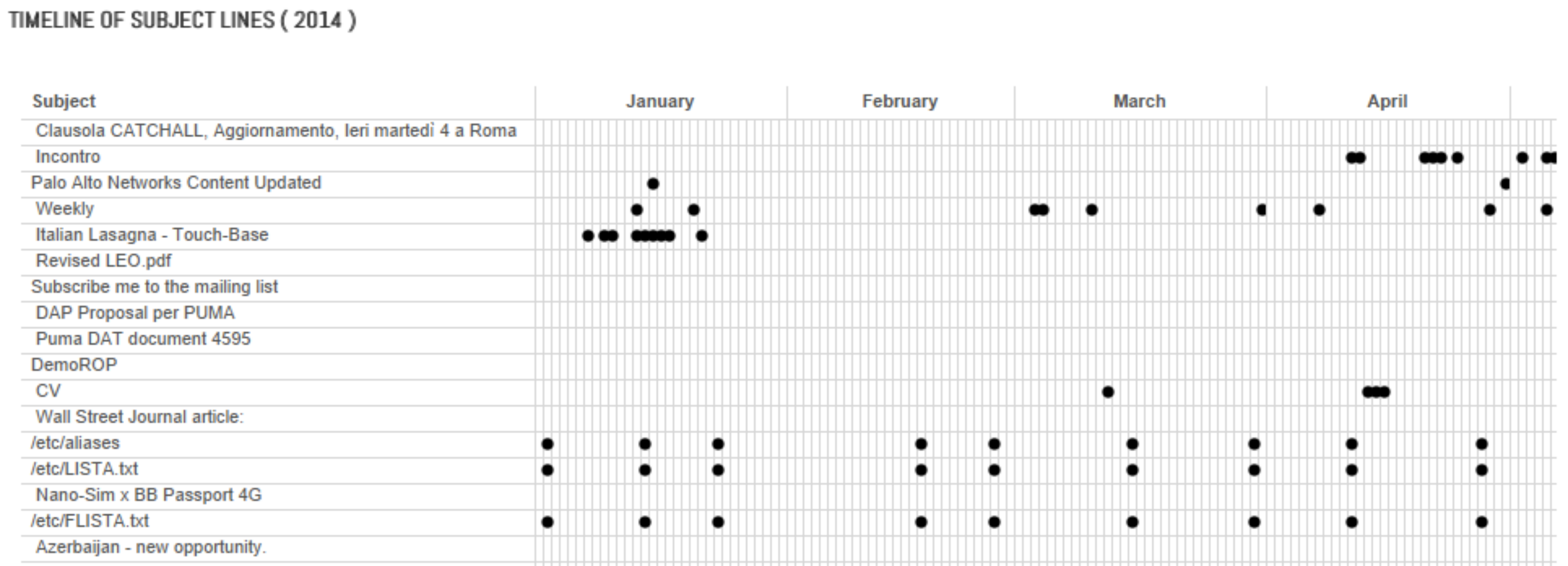


- https://labs.rs/en/metadata/



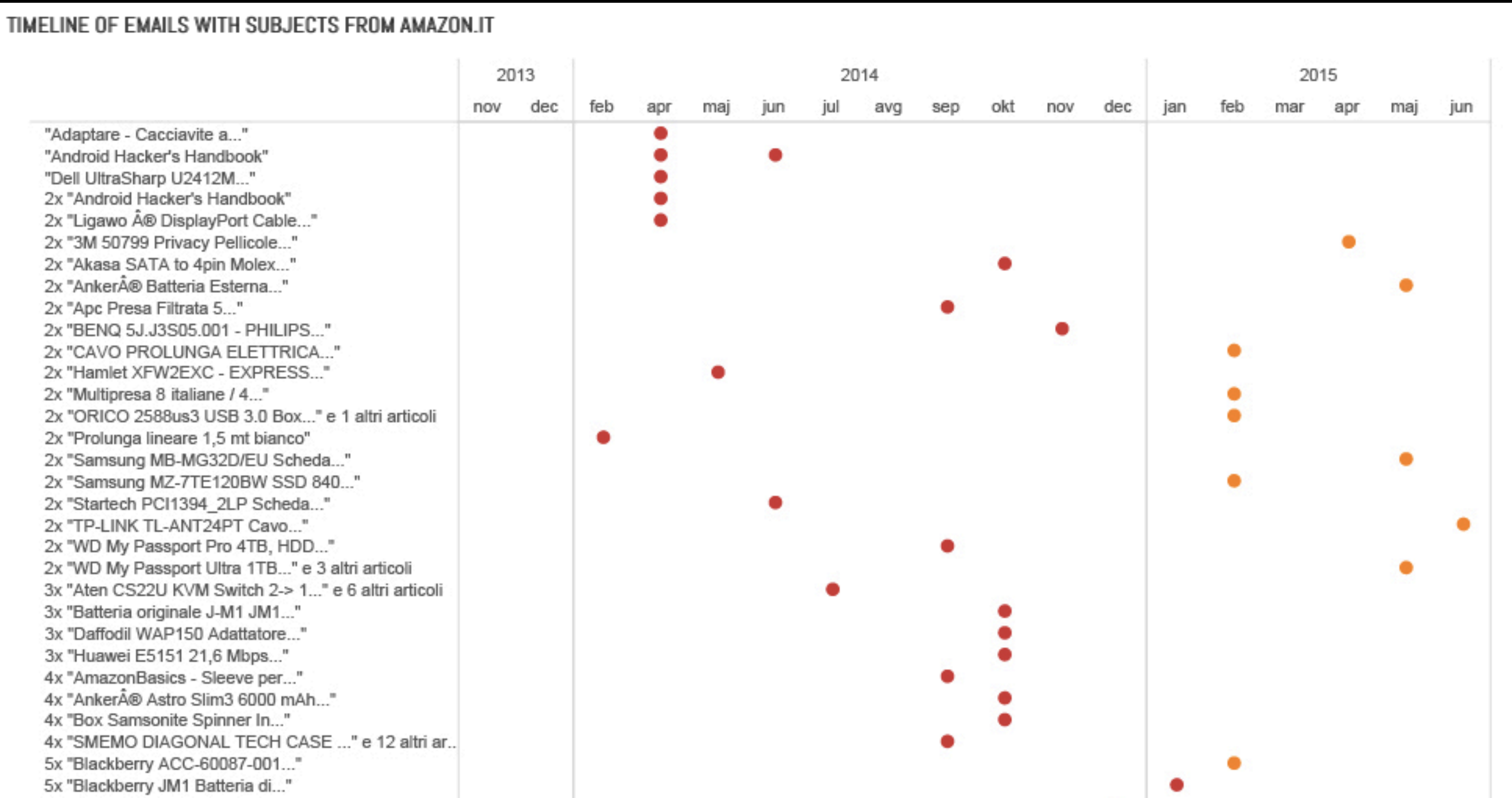
TIMELINE OF INDIVIDUAL COMMUNICATION OF EXTERNAL CONTACTS AND HT EMPLOYEES (2014-2015)

- https://labs.rs/en/metadata/



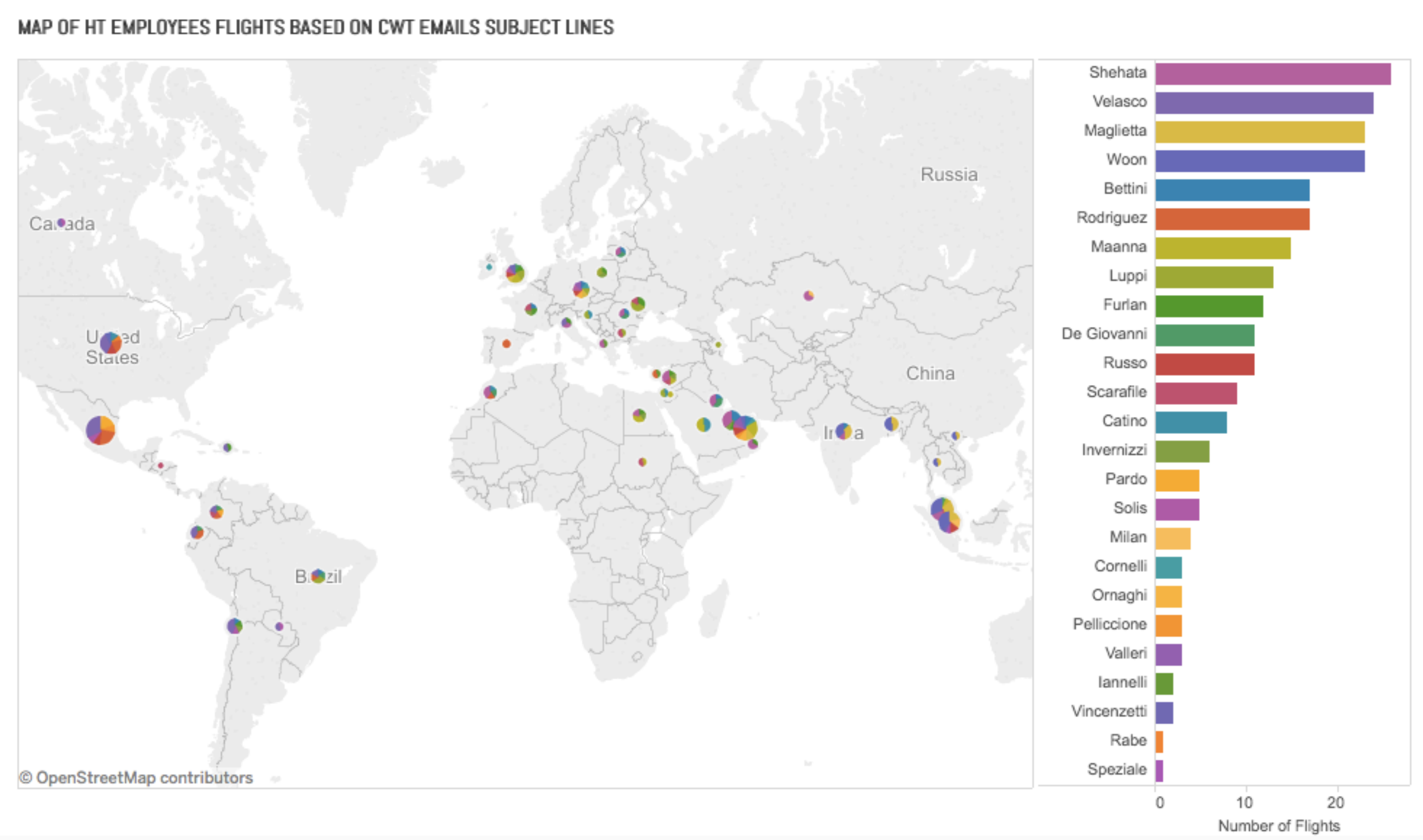
TIMELINE OF SUBJECT LINES (2014)

- https://labs.rs/en/metadata/



TIMELINE OF EMAILS WITH SUBJECTS FROM AMAZON.IT

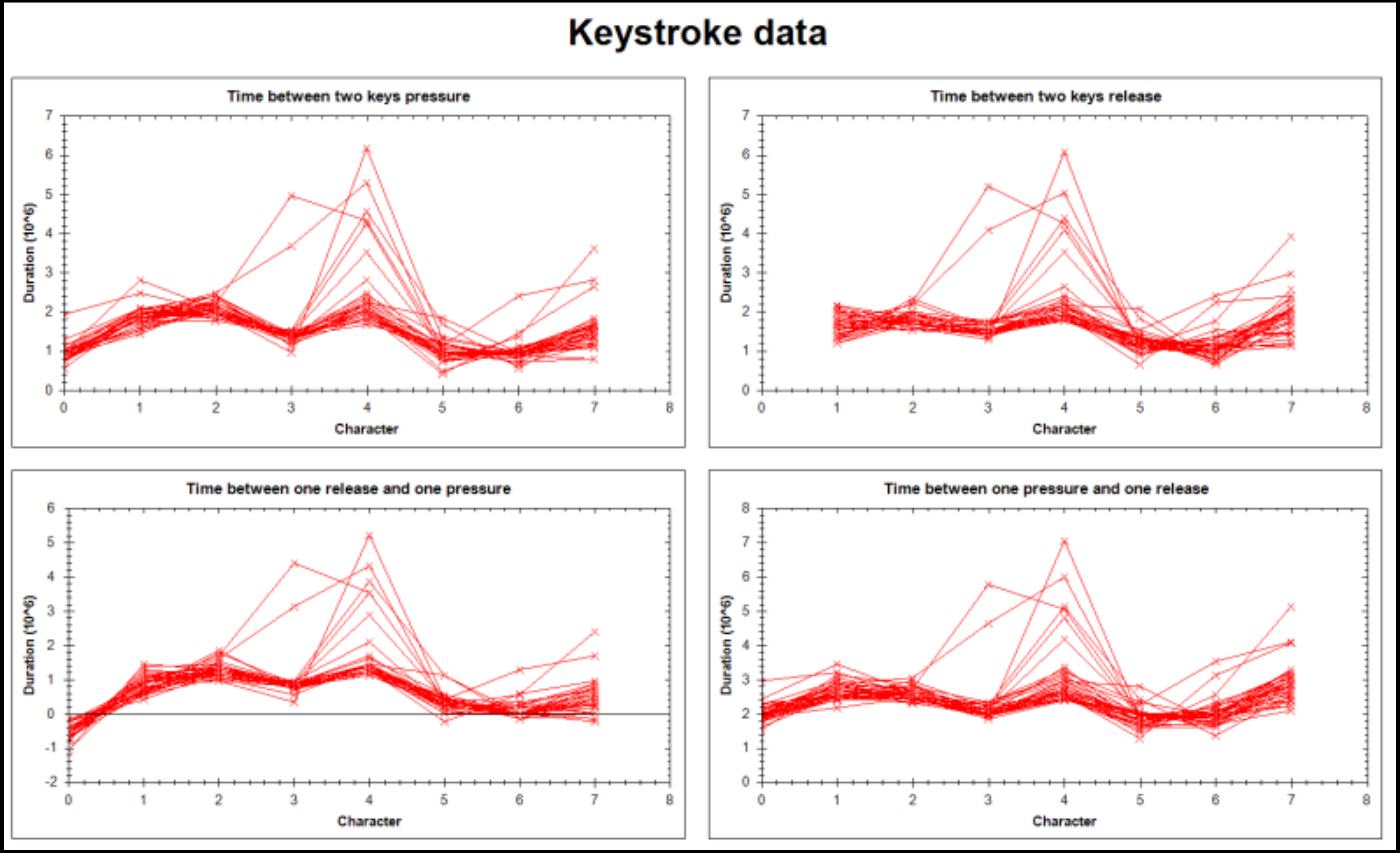
- https://labs.rs/en/metadata/



MAP OF HT EMPLOYEES FLIGHTS BASED ON CWT EMAILS SUBJECT LINES

- https://labs.rs/en/metadata/

How the way you type can shatter anonymity 1/2

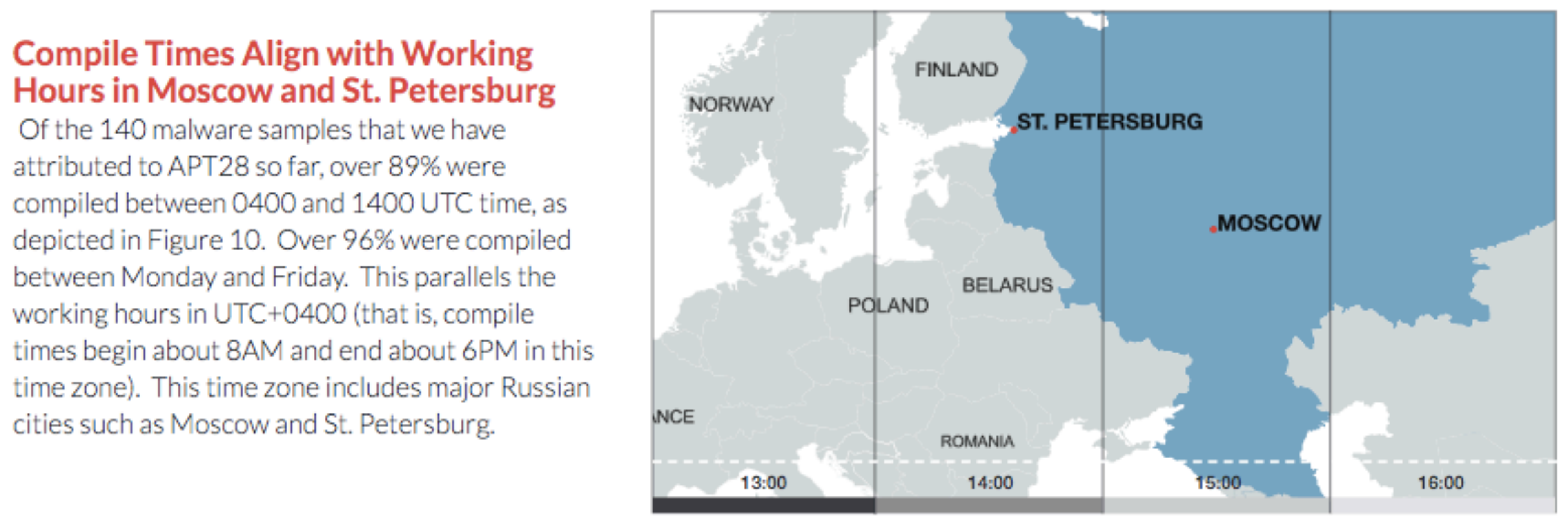


- http://arstechnica.com/security/2015/07/how-the-way-you-type-can-shatter-anonymity-even-on-tor/

How the way you type can shatter anonymity 2/2

- “The technique collects user keystrokes as an individual enters usernames, passwords, and other data into a website. After a training session that typically takes less than 10 minutes, the website—or any other site connected to the website—can then determine with a high degree of certainty when the same individual is conducting subsequent online sessions.”
- “The real concern with behavioral profiling is when it is being done by multiple big websites owned by the same company or organization. The risk to anonymity and privacy is that you can profile me and log what I am doing on one page and then compare that to the profile you have built on another page. Suddenly, the IP address I am using to connect to these two sites matters much less.”
  – http://arstechnica.com/security/2015/07/how-the-way-you-type-can-shatter-anonymity-even-on-tor/

Knowing the attackers: APT28

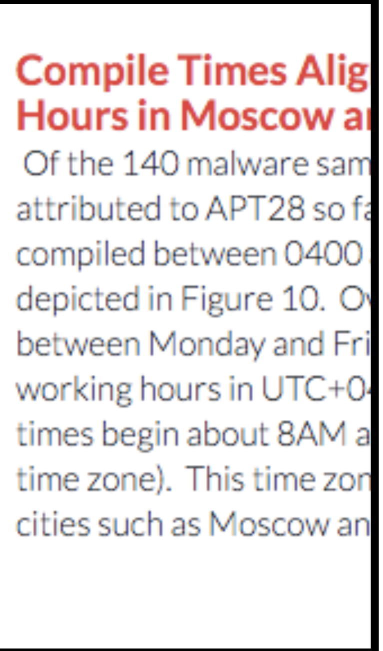


Compile Times Align with Working Hours in Moscow and St. Petersburg

Of the 140 malware samples that we have attributed to APT28 so far, over 89% were compiled between 0400 and 1400 UTC time, as depicted in Figure 10. Over 96% were compiled between Monday and Friday. This parallels the working hours in UTC+0400 (that is, compile times begin about 8AM and end about 6PM in this time zone). This time zone includes major Russian cities such as Moscow and St. Petersburg.

- https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

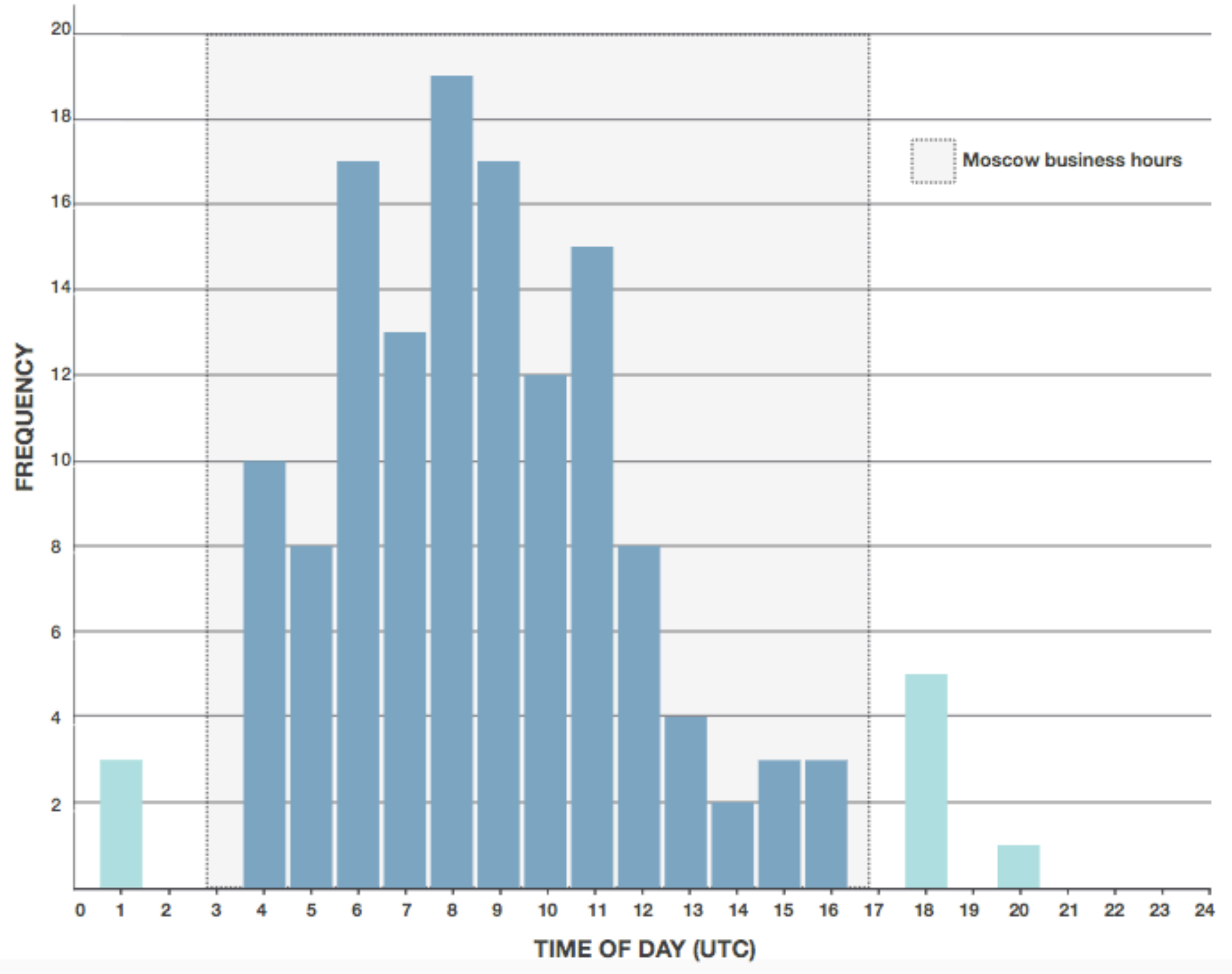
Knowing the attackers: APT28



Compile Times Alig
Hours in Moscow a

Of the 140 malware sam
attributed to APT28 so fa
compiled between 0400
depicted in Figure 10. O
between Monday and Fri
working hours in UTC+0
times begin about 8AM a
time zone). This time zo
cities such as Moscow an

Figure 10: Compile Times of APT28 malware in UTC Time



- https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

Tracking Metro Riders Using Accelerometers

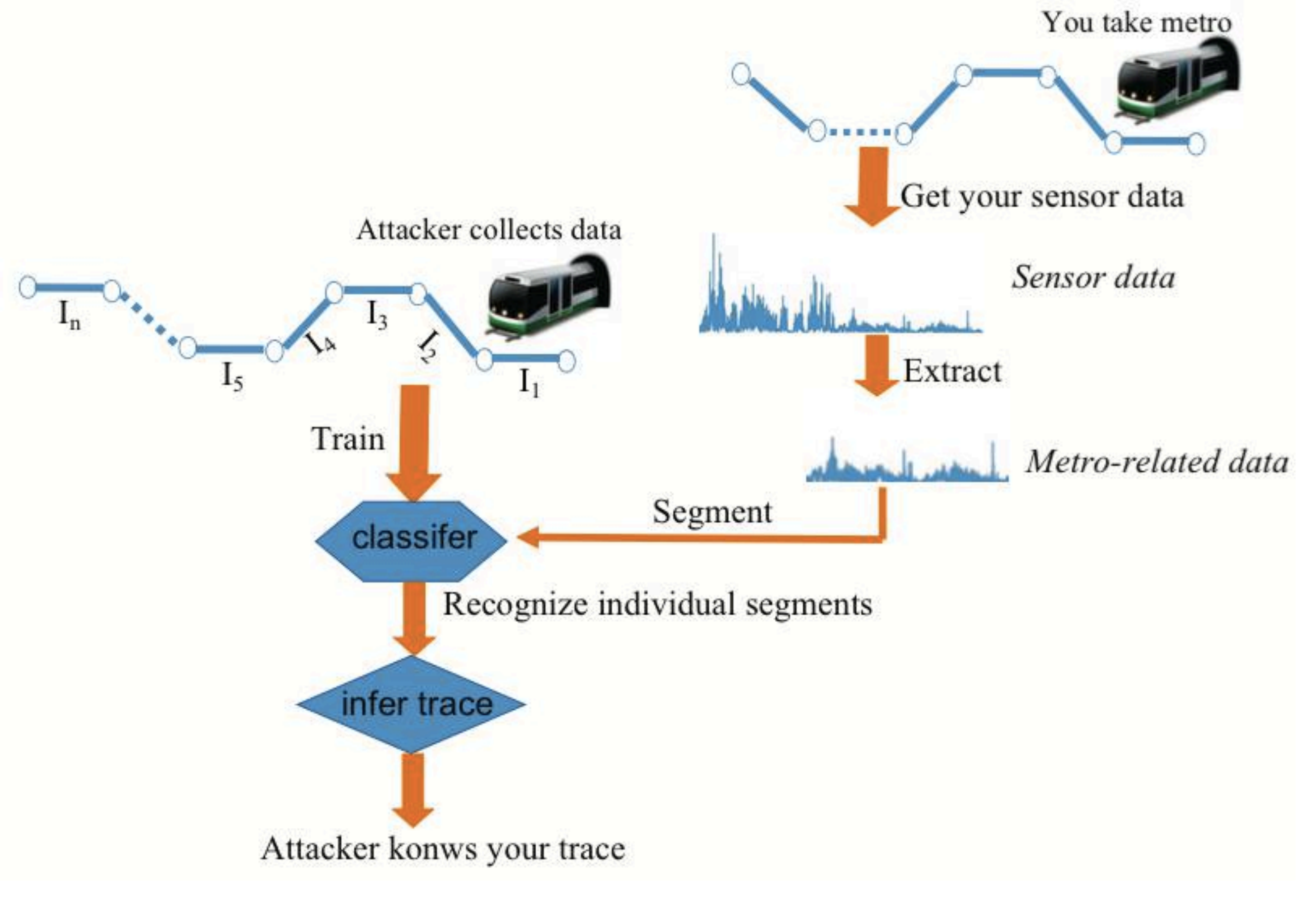
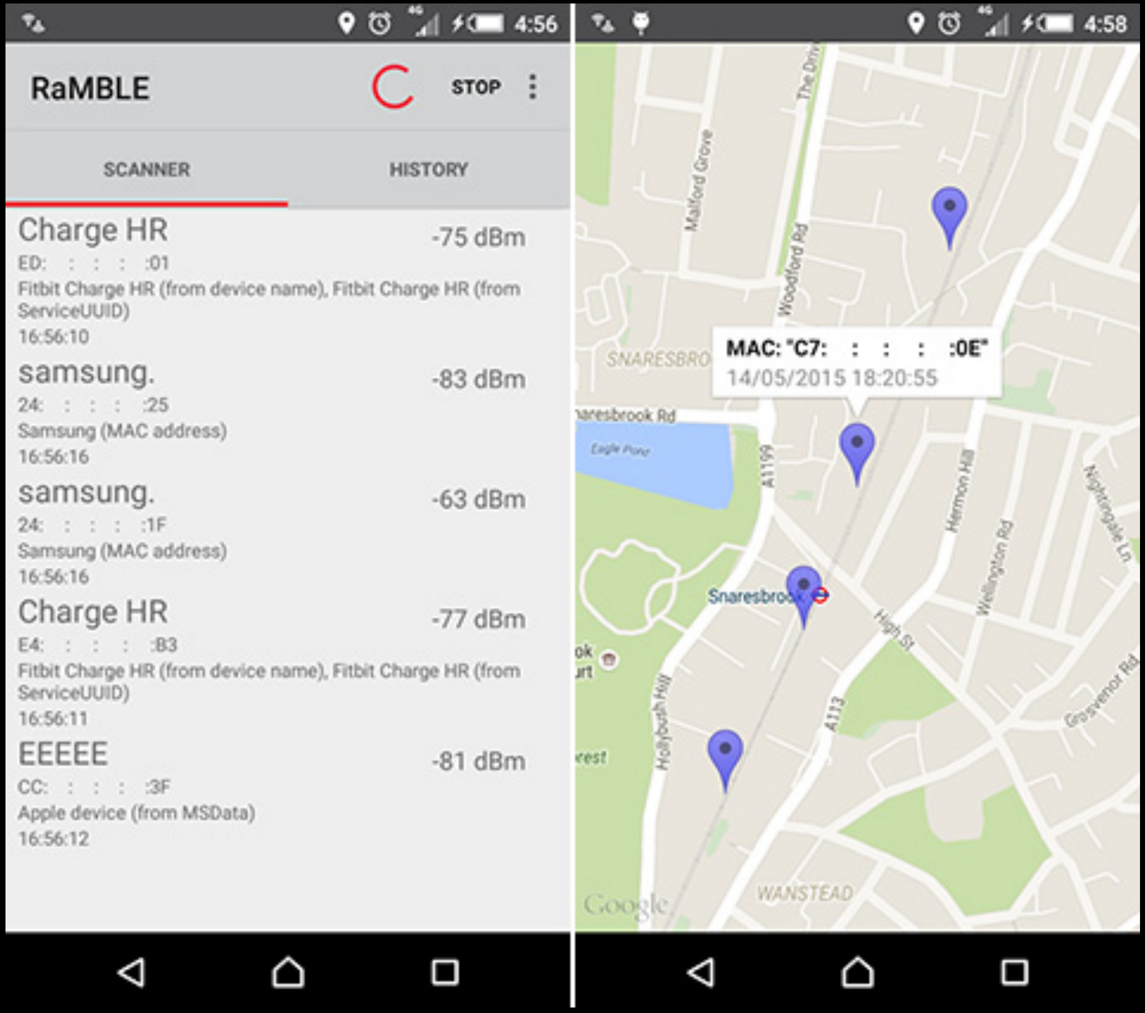


Figure 1: attack model

- http://www.theregister.co.uk/2015/05/26/tracking_metro_riders_using_accelerometers_on_smartphones/?mt=1462545176702

Sniffing and tracking wearable tech and smartphones

- “Researchers at Context Information Security have demonstrated how easy it is to monitor and record Bluetooth Low Energy signals transmitted by many mobile phones, wearable devices and iBeacons, including the iPhone and leading fitness monitors, raising concerns about privacy and confidentiality. ”



4:56

RaMBLE STOP

SCANNER HISTORY

Charge HR -75 dBm
ED: : : : :01
Fitbit Charge HR (from device name), Fitbit Charge HR (from ServiceUUID)
16:56:10

samsung. -83 dBm
24: : : : :25
Samsung (MAC address)
16:56:16

samsung. -63 dBm
24: : : : :1F
Samsung (MAC address)
16:56:16

Charge HR -77 dBm
E4: : : : :B3
Fitbit Charge HR (from device name), Fitbit Charge HR (from ServiceUUID)
16:56:11

EEEEE -81 dBm
CC: : : : :3F
Apple device (from MSData)
16:56:12

4:58

MAC: "C7: : : : :0E"
14/05/2015 18:20:55

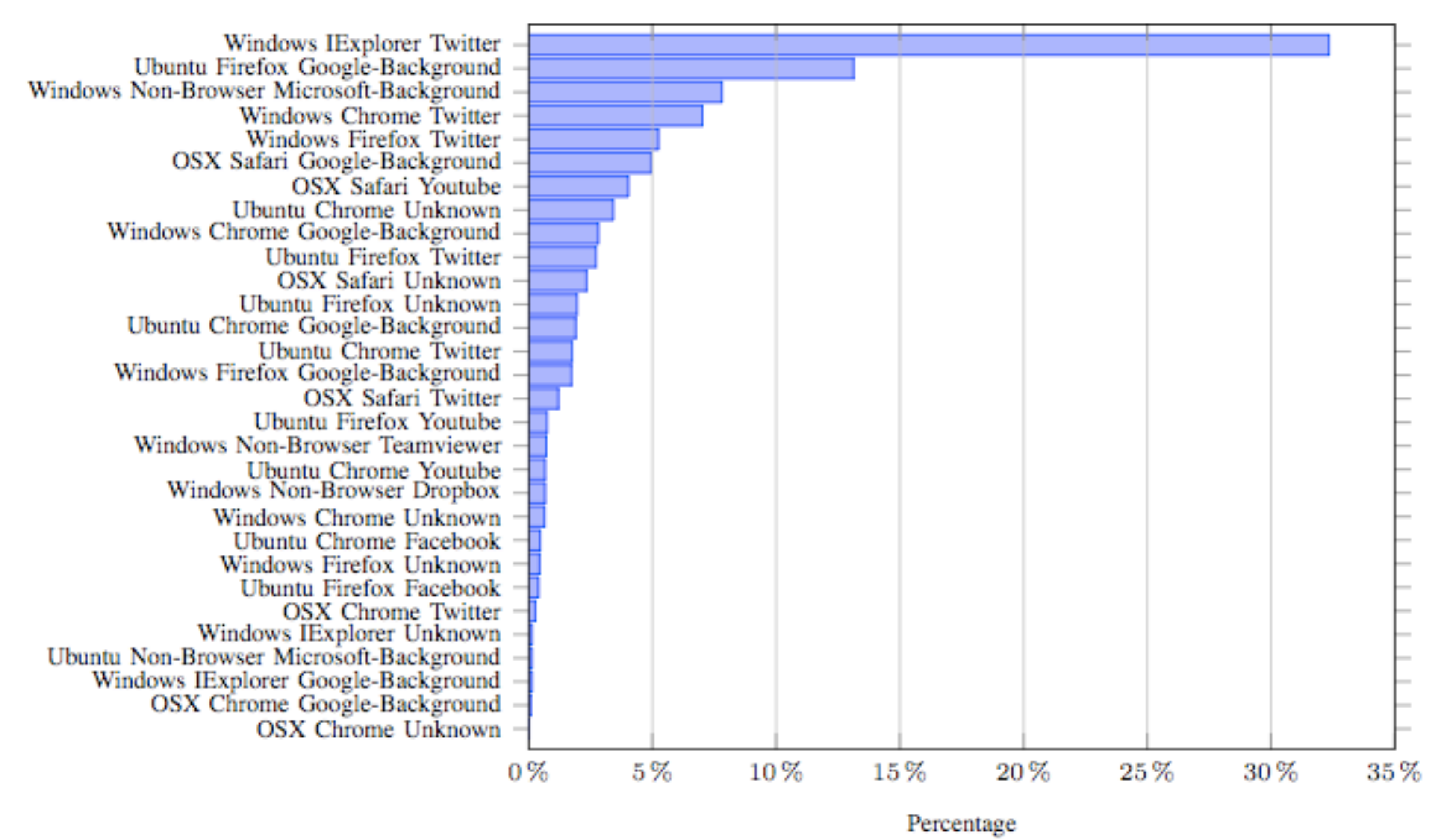
- https://www.helpnetsecurity.com/2015/05/25/sniffing-and-tracking-wearable-tech-and-smartphones/

Location determination techniques

- Examples:
  - WIFI related data can be used to determine your location. You only need to match MAC addresses with a map of known Access Points.
  - Battery consumption can be used to identify your movements
  - It might be obvious but apps for taxi services/maps/health etc.. could have a history of your preferred places.

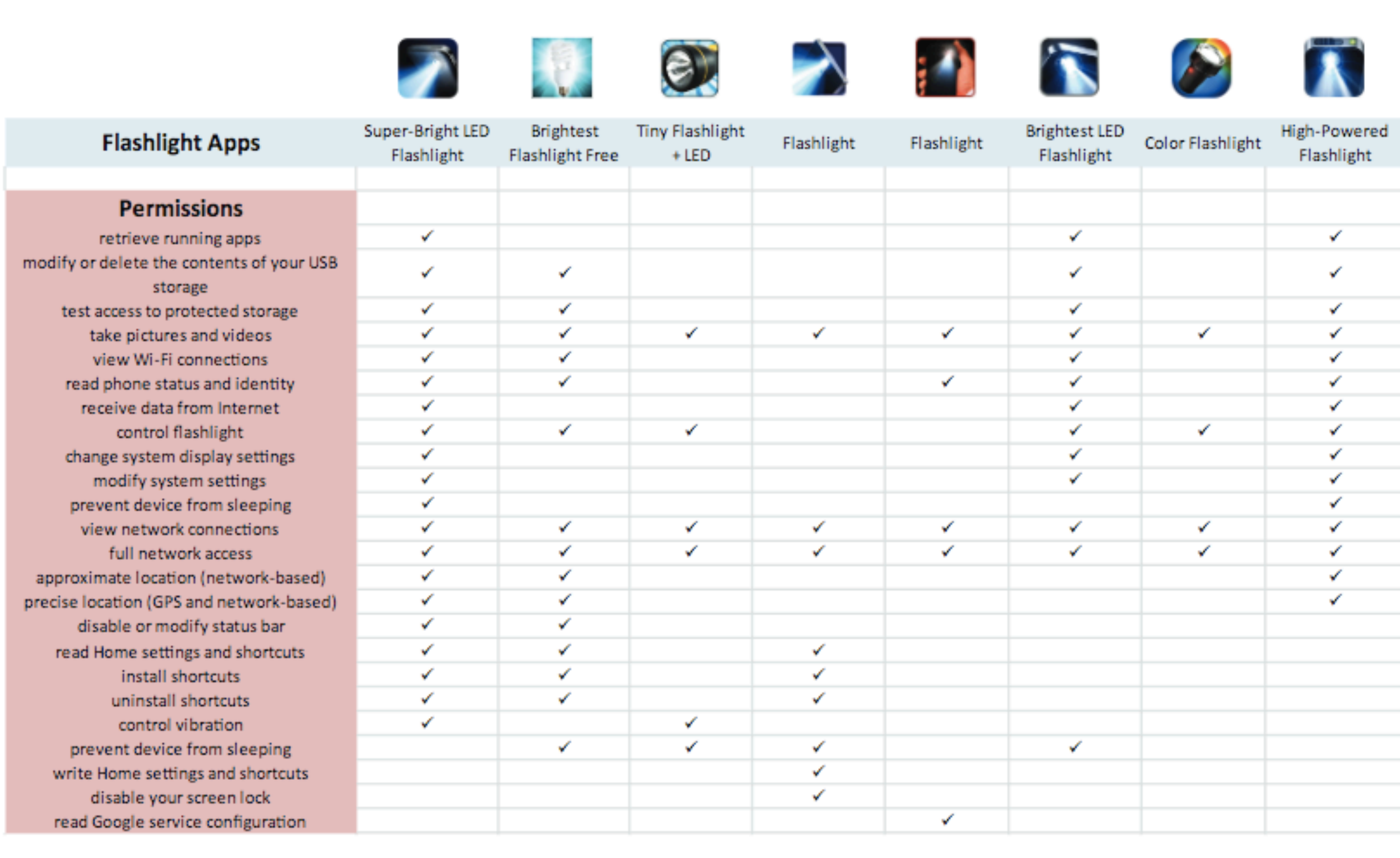
- http://www.zdnet.com/article/how-google-and-everyone-else-gets-wi-fi-location-data/
- http://www.theregister.co.uk/2015/02/23/mobe_battery_stats_the_latest_tracking_trick_for_spies_creeps/
- http://www.ibtimes.com/spying-celebrities-nyc-taxi-metadata-exposes-celeb-locations-strip-club-clients-1696744?rel=rel1

Analyzing HTTPS Encrypted Traffic to Identify User's Operating System, Browser and Application



- http://arxiv.org/ftp/arxiv/papers/1603/1603.04865.pdf

Check!



Flashlight Apps	Super-Bright LED Flashlight	Brightest Flashlight Free	Tiny Flashlight + LED	Flashlight	Flashlight	Brightest LED Flashlight	Color Flashlight	High-Powered Flashlight
Permissions								
retrieve running apps	✓					✓		✓
modify or delete the contents of your USB storage	✓	✓				✓		✓
test access to protected storage	✓	✓				✓		✓
take pictures and videos	✓	✓	✓	✓	✓	✓	✓	✓
view Wi-Fi connections	✓	✓				✓		✓
read phone status and identity	✓	✓			✓	✓		✓
receive data from Internet	✓					✓		✓
control flashlight	✓	✓	✓			✓	✓	✓
change system display settings	✓					✓		✓
modify system settings	✓					✓		✓
prevent device from sleeping	✓							✓
view network connections	✓	✓	✓	✓	✓	✓	✓	✓
full network access	✓	✓	✓	✓	✓	✓	✓	✓
approximate location (network-based)	✓	✓						✓
precise location (GPS and network-based)	✓	✓						✓
disable or modify status bar	✓	✓						
read Home settings and shortcuts	✓	✓		✓				
install shortcuts	✓	✓		✓				
uninstall shortcuts	✓	✓		✓				
control vibration	✓		✓					
prevent device from sleeping		✓	✓	✓		✓		
write Home settings and shortcuts				✓				
disable your screen lock				✓				
read Google service configuration					✓			

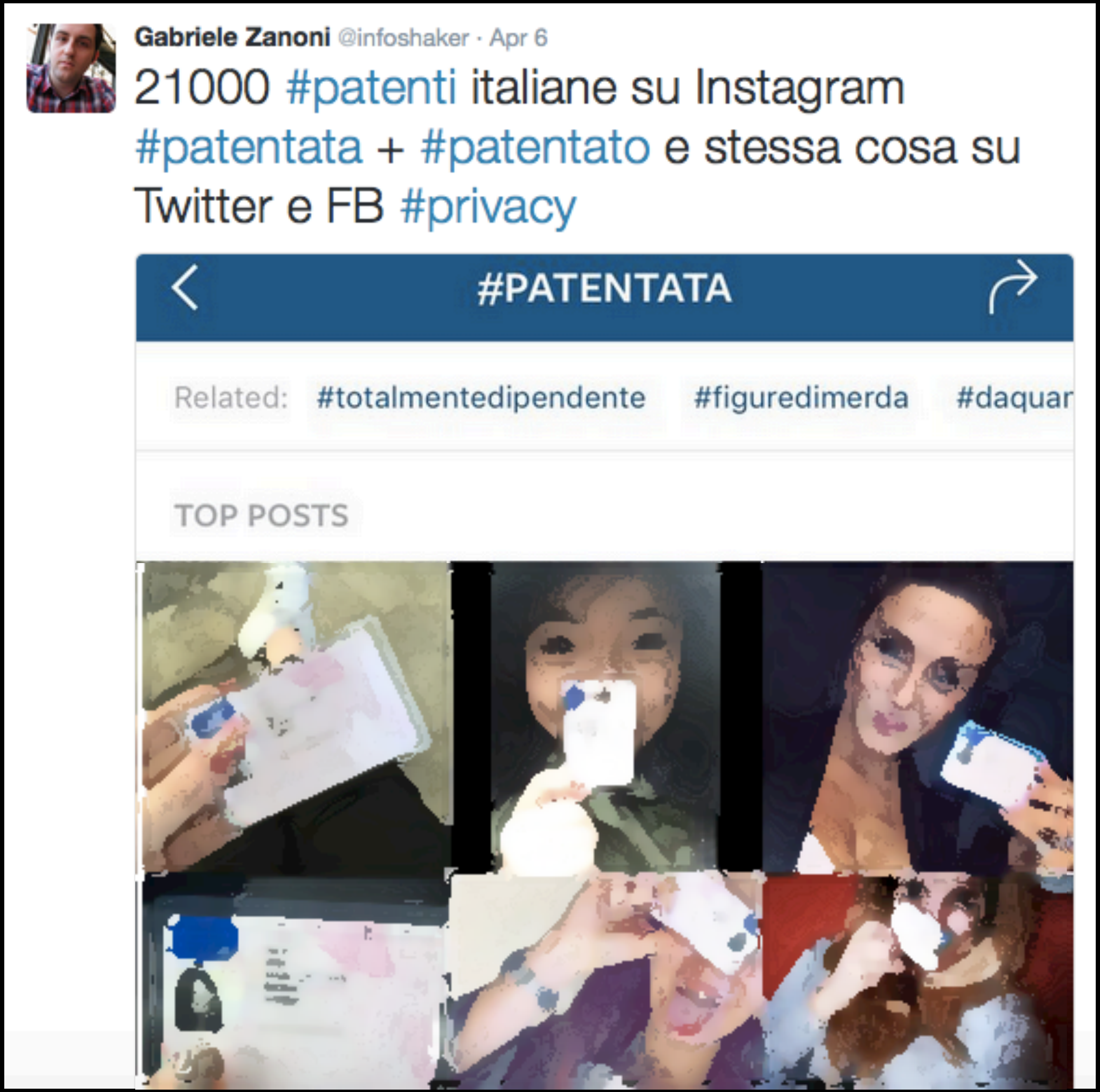
Full report:
http://www.snoopwall.com/wp-content/uploads/2014/10/Flashlight-Spyware-Appendix-2014.pdf

Summary

Summary

- Pay attention to information we leave or share on the Internet every day
- Evaluate the usage of apps with a low number of requirements in terms of permissions
- Giving too many privileges or too much information to app/service providers might imply that when a company get hacked then the attackers could have access to our sensitive details

Really!1! - Pay Attention



Gabriele Zanoni @infoshaker · Apr 6

21000 #patenti italiane su Instagram #patentata + #patentato e stessa cosa su Twitter e FB #privacy

Thank you!

Gabriele Zanoni
@infoshaker