Motivation

Vulnerability

> A **flaw or weakness in system** security procedures, design, implementation, or internal controls **that could [...] result in a security breach** or a violation of the system's security policy [^1]

Exploit

> A piece of software, a chunk of data, or a sequence of commands that **takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior** to occur on computer software, hardware, or something electronic (usually computerized) [^2]

Zero-Day

> **A zero day vulnerability** refers to a hole in software that **is unknown to the vendor**.
>
> This security hole is then **exploited by hackers before the vendor becomes aware** and hurries to fix it—this exploit is called a zero day attack. [...]
>
> The term **“zero day” refers to the unknown nature** of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users. [^3]

Exercise 1.1

Brainstorming Attackers

1. Identify and 🖍️ a mind map of possible **Attackers**
2. Rate the danger posed by each attacker type (💀 to 💀💀💀)
3. Estimate the risk of your own employer being targeted by each identified attacker type (in %)
4. Which attacker types are likely to work together and how does this impact their danger rating?

Attacker Stereotypes

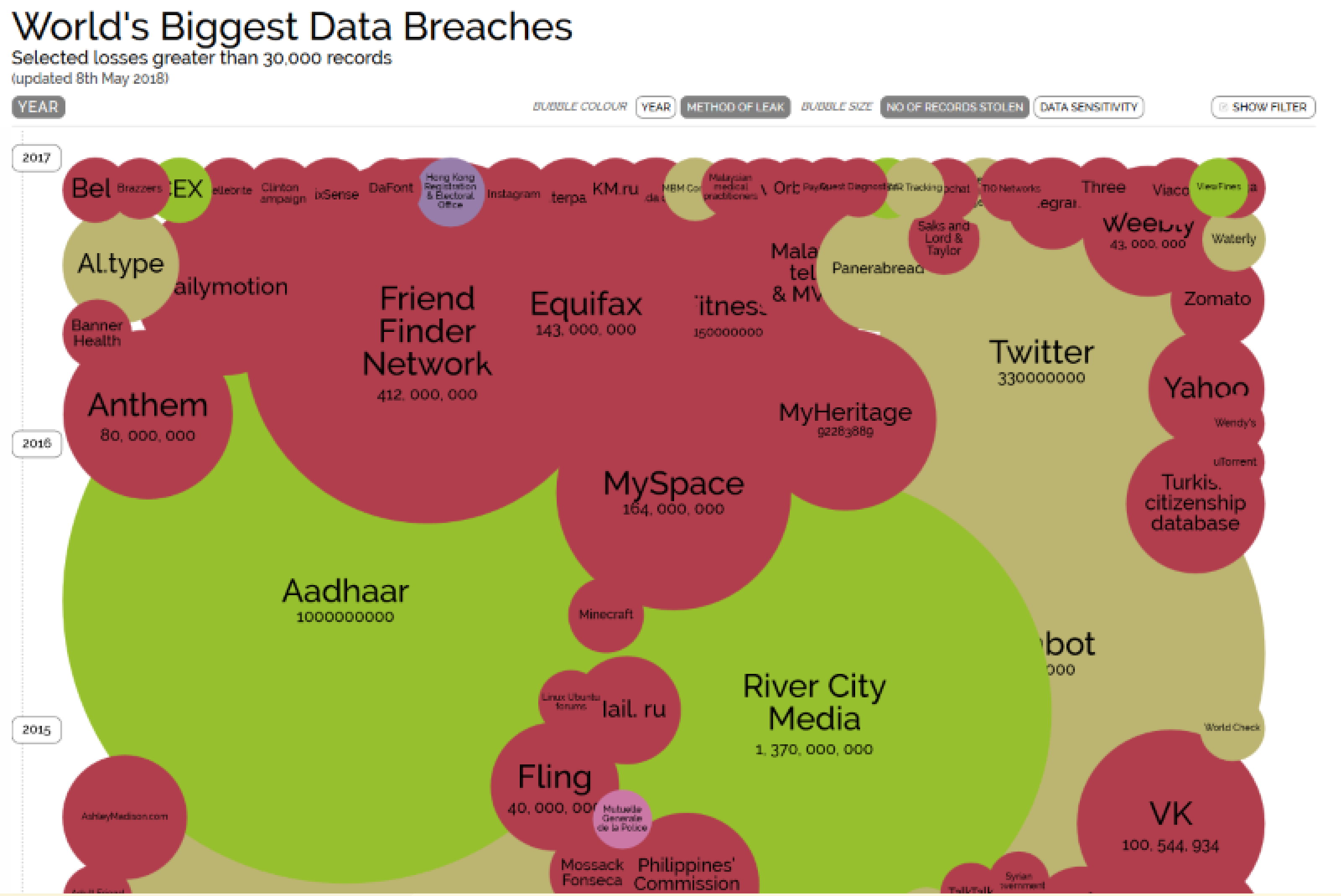
Name	Characteristics	Danger
Script Kiddie	Bragging rights & wreaking havoc	💀
Hacktivists	(Pseudo-)political / social motivation	💀💀
Competitors	Industrial Espionage	💀💀
Organized Crime	Monetization, Cyber-Crime-as-a-Service	💀💀
Evil Employees	Dangerous insider knowledge	💀💀💀
Nation States	Unlimited resources and budget	💀x100

Advantage of the Attacker

- Attacker must **succeed once**
  - Defender must get it right *all the time*
- Attacker can choose the **weakest spot**
  - Defender must defend *all places*
- Attacker can leverage **zero-days**
  - Defender can only defend against *known attacks*
- Attacker can **play dirty**
  - Defender needs to *play by the rules*

Case Studies

Data Breaches (by no. of records)

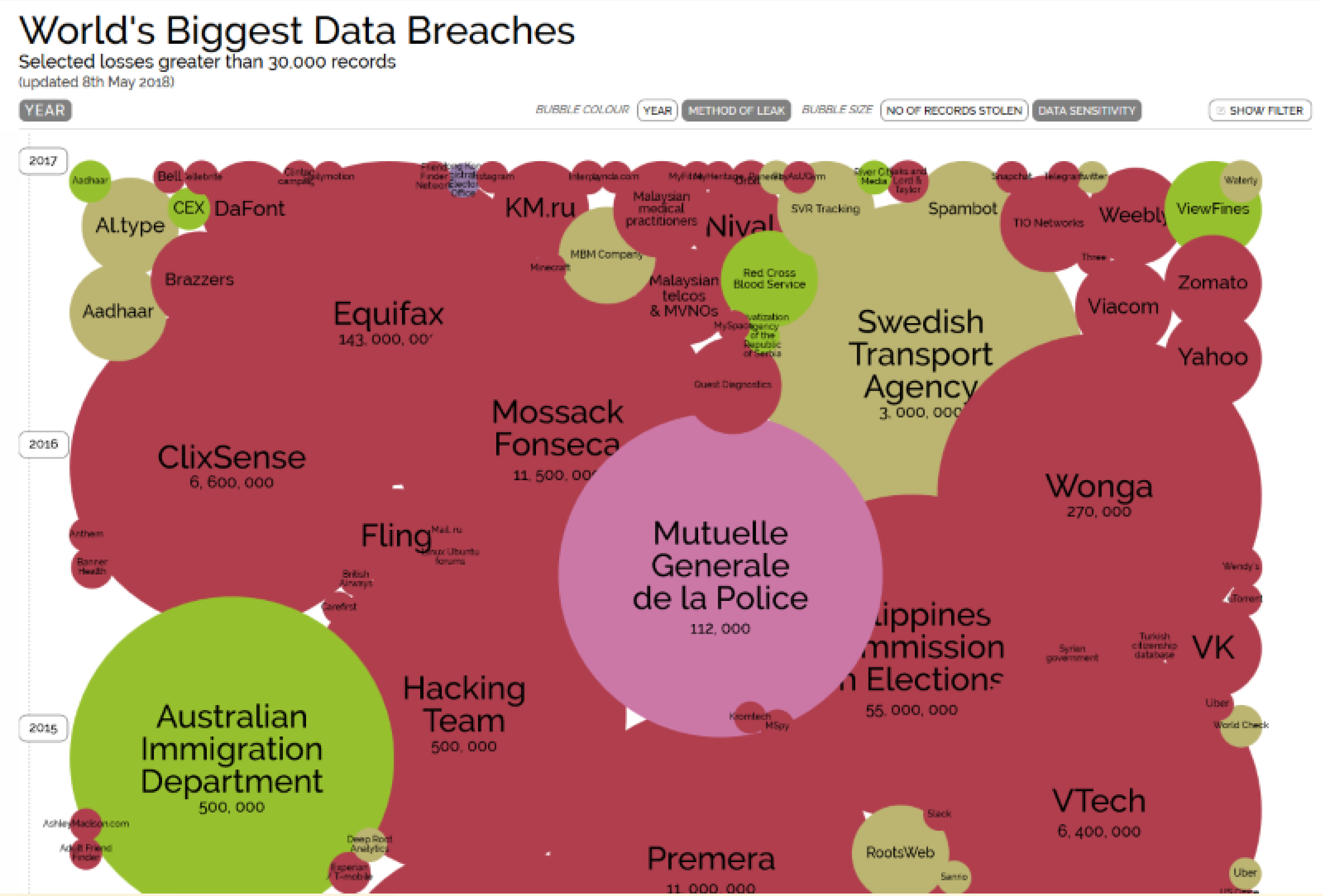


World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 8th May 2018)

Data Breaches (by data sensitivity)



World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 8th May 2018)

Aadhaar (January 2018)

> Today, The Tribune “purchased” a service being offered by anonymous sellers over WhatsApp that provided unrestricted access to details for any of the more than 1 billion Aadhaar numbers created in India thus far. [^4]

> It took just Rs 500, paid through Paytm, and 10 minutes in which an “agent” of the group running the racket created a “gateway” for this correspondent and gave a login ID and password [...] and instantly get all particulars that an individual may have submitted to the UIDAI (Unique Identification Authority of India), including name, address, postal code (PIN), photo, phone number and email.
>
> What is more, The Tribune team paid another Rs 300, for which the agent provided “software” that could facilitate the printing of the Aadhaar card after entering the Aadhaar number of any individual. [^4]

***Sidenote:** 800 Indian Rupee equals 10.04 Euro (28.06.2018)* 💸

Equifax (September 2017)

> If you have a credit report, there’s a good chance that you’re one of the 143 million American consumers whose sensitive personal information was exposed in a data breach at Equifax, one of the nation’s three major credit reporting agencies. [^5]

> Here are the facts, according to Equifax. The breach lasted from mid-May through July. The hackers accessed people’s names, Social Security numbers, birth dates, addresses and, in some instances, driver’s license numbers. They also stole credit card numbers for about 209,000 people and dispute documents with personal identifying information for about 182,000 people. And they grabbed personal information of people in the UK and Canada too. [^5]

***Sidenote:** Recommended steps for protection include "monitor your existing credit card and bank accounts closely" but also "consider placing a credit freeze" 🍦 or "placing a fraud alert on your files".*