FRI

UNIVERZA V LJUBLJANI | Fakulteta za računalništvo in informatiko

Digital Forensics: INFOSEC foundations

doc. dr. David Modic

14.03.2025

Outline

UL | FRI

- Who am I and why am I messing with your morning
- State of play, currently
- Terminology
- Examples
- Discussion

- **We need to finish by 9:55**

Who am I?

UL | FRI

- doc. dr. David Modic, an economic psychologist.
- Assistant professor at FRI.
- Director of studies for vocational program BVS-RI.
- Researcher and principal investigator at FRI.
- Senior Non-Residential Member King's College, Cambridge
- Previously:
- Researcher at the Computer Laboratory, Cambridge University.
- Deputy Head CamCERT (social engineering).
- Consultant (NATO, Brazillian Government, Japanese Police, UK Government, MOD Lithuania…)

In practice, I deal with security incidents, research which mechanisms work well in social engineering, and what kind of people hackers are. My colleagues and me run hacking exercises, penetration tests, and training courses for companies.
I teach a PhD INFOSEC module at FRI.

david.modic@fri.uni-lj.si

INFOSEC (losses)

UL | FRI

- (Quiz) How big are the losses to cyber attacks? Give me a guess.
  - These are all good numbers. As good as most of the predictions floating around ☺.
  - A trick question.
  - Short answer: *No one knows*.
  - Longer answer: *Depends on how you calculate them (cf. e.g. Anderson, et al., 2012)*

david.modic@fri.uni-lj.si

INFOSEC (likelihood of a breach)

UL | FRI

- **(Quiz)** How likely is it that any given entity that has some utility will be breached at some point in time?
  - That's right, it is roughly 100% give or take.
- **(Quiz)** What does severity of the breach depend on?
  - Yes, it depends on **(a)** preparation, and **(b)** post festum handling.

david.modic@fri.uni-lj.si

INFOSEC (likelihood of a breach)

UL | FRI

- (Quiz) What are the some of bigger flaws of cyber defense? Speculate, please.
  - Reacting not acting. See shoes and airports, for example.
  - Ignoring typical patterns (e.g. misdirection – cf. NATO Locked Shields 2019 trial run).
  - Focusing on wrong attack vectors (see next slide).

david.modic@fri.uni-lj.si

INFOSEC (common features of breaches)

UL | FRI

(Quiz) Do you think black hats go in blind? **Yes / No**?

No, they don't. Typically, they will spend weeks or months gathering data.

(Quiz) Will they attack only a single point of failure?

No, they won't. See Locked Shields 2019. Misdirection!

(Quiz) Will they tailor the attack to the target?

Yes and no. The run of the mill lower value scatter-gun targets, no. High value targets, yes, for sure.

david.modic@fri.uni-lj.si

Intelligence (OSINT)

UL | FRI

- (Quiz) What is OSINT?
  - Open Source INTelligence. What does that mean?
  - Information that is gathered from overt, publicly available sources.
- (Quiz) Does the word 'open' refer to open-source in this context?
  - NO. it just means the information is *open* to everyone to see.
- Six categories: offline media, online, government data, academic publications, commercial data, 'grey literature'.

david.modic@fri.uni-lj.si

Basic security terms – Threat Model

UL | FRI

- (Quiz) What is a Threat Model?
  - Essentially, an action plan with priorities. What will an attacker do, which vulnerabilities will they attack first, what are they hoping to achieve.
  - When I asked you in Homework 1, to provide the reasoning for your target choice, I was pushing you to do threat modelling.
  - We are all constantly threat modelling: how to avoid a long line at the cafeteria, how to drive along a route where there are less traffic delays, etc. We predict a possible threat, assess the severity, take evasive action and proceed with the plan.

david.modic@fri.uni-lj.si

Basic security terms – Attack vector

UL | FRI

- (Quiz) What is an Attack Vector?
  - The means by which an attacker gains access to infrastructure.
  - Could be human based – social engineering, phishing, extortion, …
  - or mechanical – malware, viruses, 0-day exploits
- (Quiz) In practice, which is more successful mechanical or human?
  - That is right, human attack vectors (I'll give you some examples later).

david.modic@fri.uni-lj.si

Attack vectors – M or H?

UL | FRI

- (Quiz) Which Attack Vectors are more common (Mechanical or Human based)?
  - Mechanical.
- (Quiz) Which are more effective?
  - Human based (*cf.* Cambridge netflow logs).

david.modic@fri.uni-lj.si

Attack vectors – M or H?

- (Quiz) Why are human attack vectors the most frequently abused ones?
  - They are cheaper to exploit.
  - They require less technical knowledge.
  - Attacking people exploits common misconceptions of security personnel.

david.modic@fri.uni-lj.si

UL | FRI

OSINT example

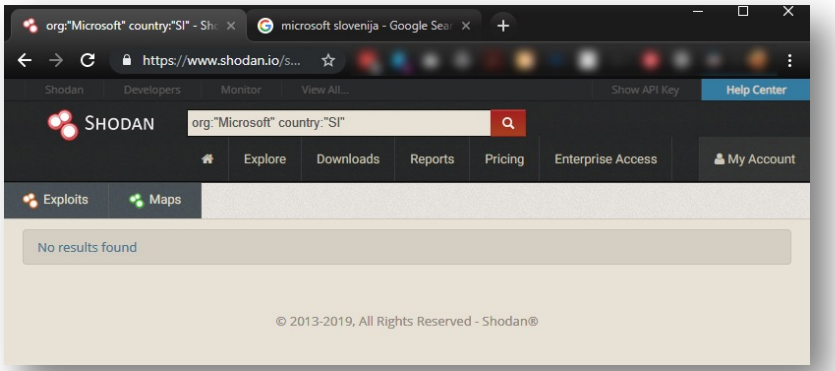
2a. OSINT example

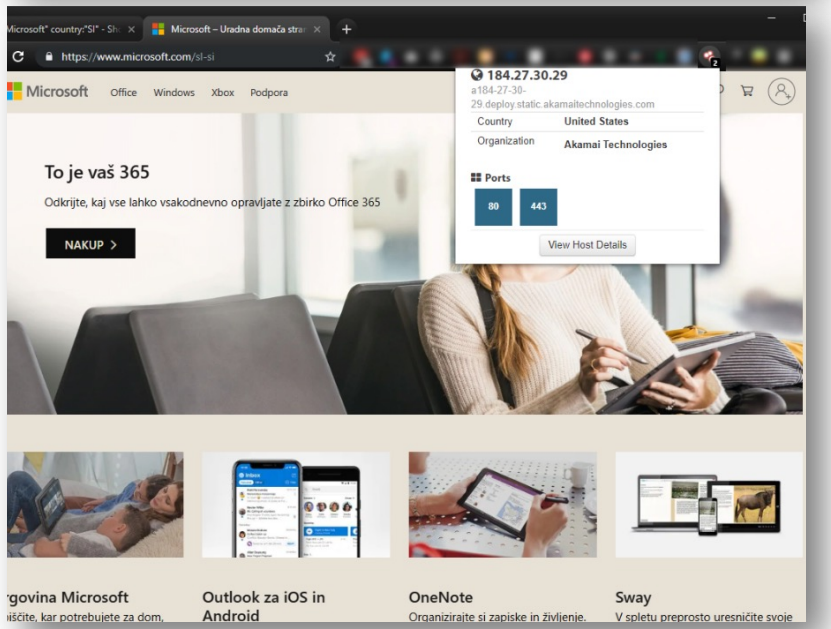
- Goal 1: I want to gain access to Microsoft Slovenia financial resources, because I want to syphon funds.
- Goal 2: I want to access Microsoft IP to (a) sell it and (b) find loopholes for further exploits.
- Attack Vectors: Mostly human, although I will do passive scanning for the hell of it.
- (Quiz) Why do I not expect to find any mechanical flaws?
  - That is right, because (a) mechanical security is usually good enough. And (b) it is usually not worth burning 0-days on attacks.

david.modic@fri.uni-lj.si

2b. Step 1: intelligence gathering

- Shodan shows that Microsoft Slovenia does not have any servers in Slovenia.
- That is further confirmed by looking with Shodan extension at the Microsoft Slovenia web page – NOT A SLOVENE IP.

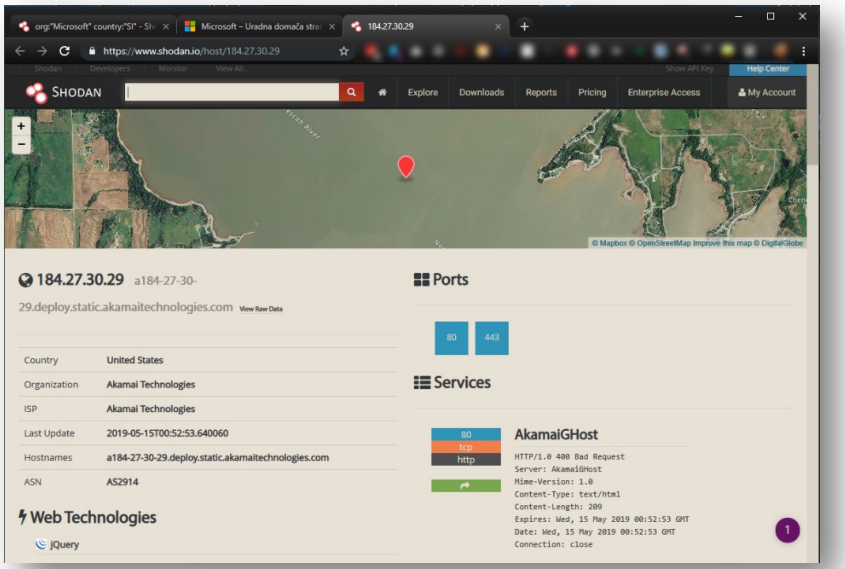


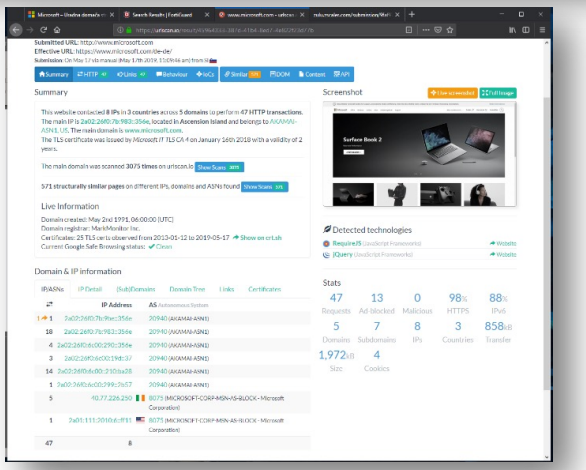


david.modic@fri.uni-lj.si

2c. Step 1: intelligence gathering II.

- Shodan host info shows that the server is nicely obfuscated – located somewhere in the ocean...
- I get some fairly useless info from urlscan. I do now know IPv6 is enabled and used by default on the MS servers.

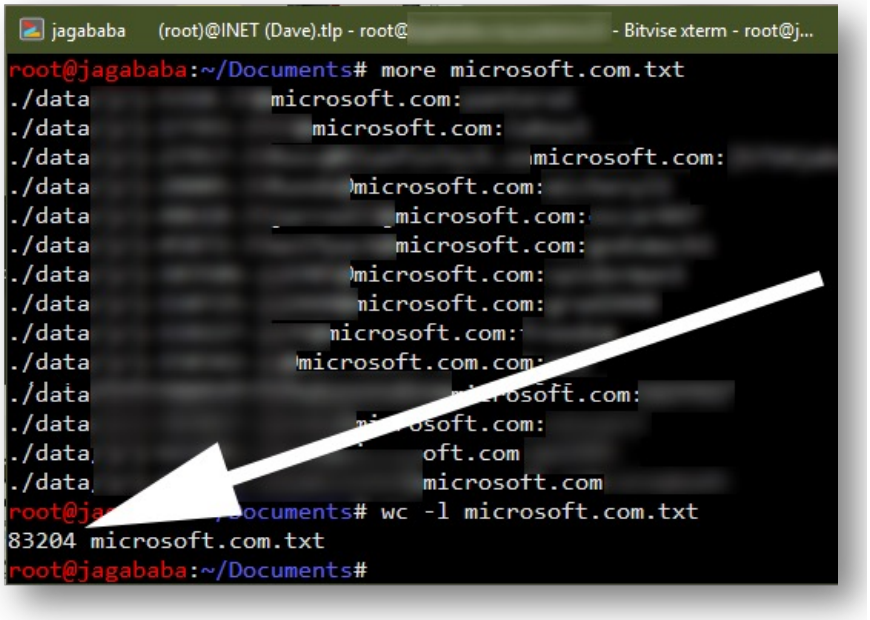




david.modic@fri.uni-lj.si

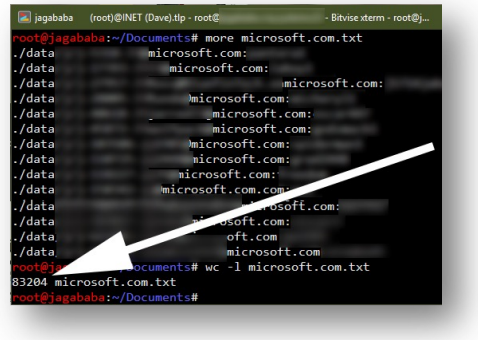
2d. Step 1: intelligence gathering III.

- What does the breach database say about microsoft.com emails?
  - *Breach DB is a database containing leaked usernames and passwords (currently I access ~1.2 billion pairs)*
- There are a bit more than 83.000 entries with the domain Microsoft.com in the email address.



david.modic@fri.uni-lj.si

2e. Step 1: intelligence gathering IV.

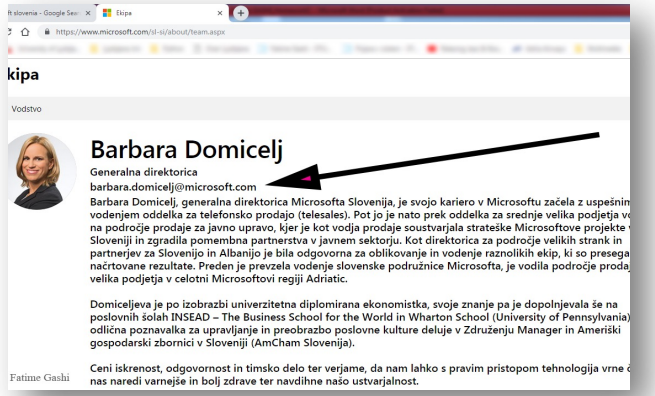


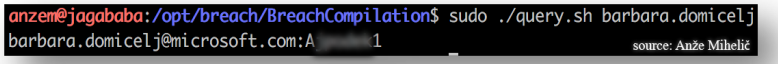
- Now. I have no idea if any passwords still work or where.
- Trying them out would be *illegal*.
- But, according to Panda Security research 67% of people use one password for everything and ~85% use the same password for all e-commerce sites.
- So, this is useful in two ways – **(a)** I know a bit about how employees construct passwords, and **(b)** there is a chance that I could log-in with this password into something valuable.

david.modic@fri.uni-lj.si

2f. Step 2: OSINT I.

- The CEO of MS.SI is Barbara Domicelj. Her email address is apparently barbara.domicelj@microsoft.si
- The breach database offers one hit.
- This is quite probably not her work account password. If it is, I despair. Eight characters, first uppercase, last is a number… Brute-force time is measured in seconds.

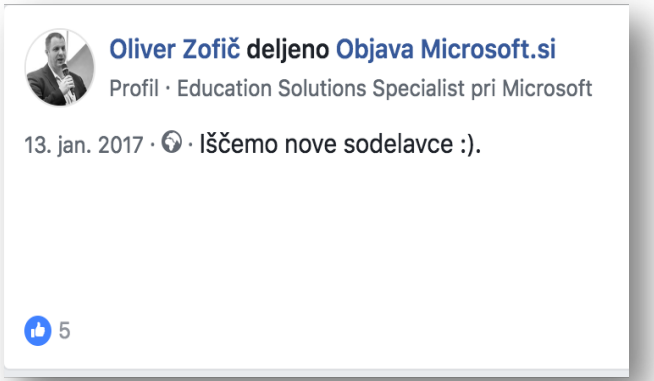




david.modic@fri.uni-lj.si

2g. Step 2: OSINT II.

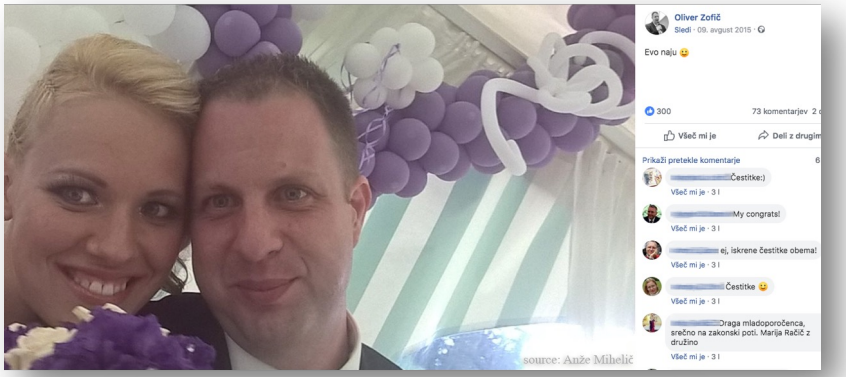
- Oliver Zofič is apparently an education solutions specialist at Microsoft Slovenia.
- He has a Facebook page, though). We find he is from Brežice, but currently lives in Ljubljana.
- The breach database offers one hit for a gmail account.

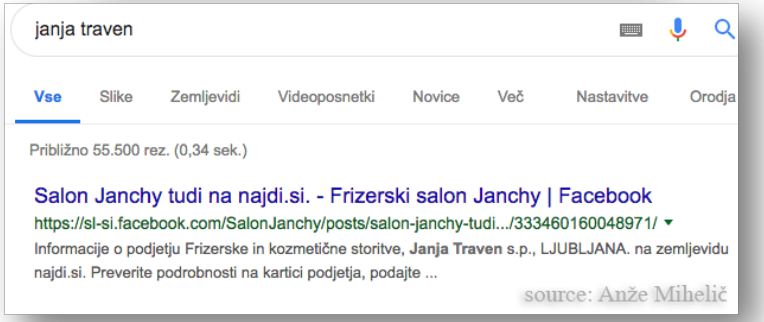


david.modic@fri.uni-lj.si

2h. Step 2: OSINT III.

- Oliver Zofič is married to Janja Zofič (August 9th 2015). They have two children, one born 8.5.2016, the other in 2018.
- Janja Zofič's maiden name is Traven.
- Janja has a hairdressing salon in Ljubljana, registered in her maiden name.

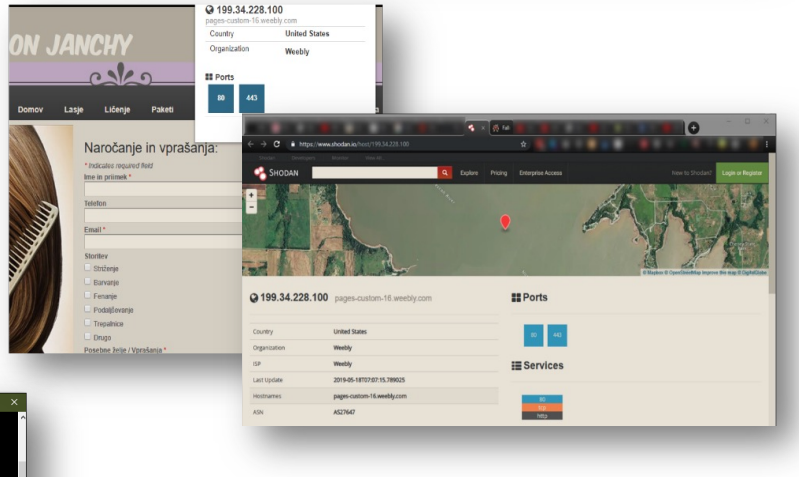


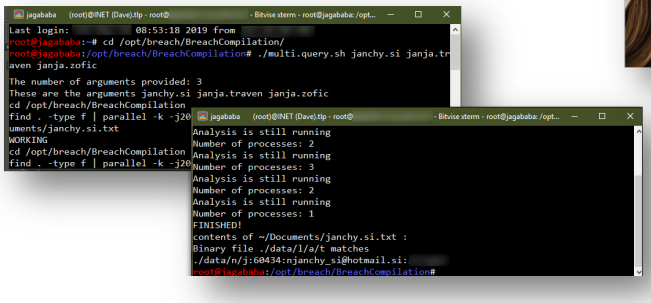


david.modic@fri.uni-lj.si

2i. Step 2: OSINT IV.

- Salon Janchy webpage yields Janja's work/contact details.
- Shodan gives potentially exploitable info.
- There is a password attached to the Salon's email in breach db.





david.modic@fri.uni-lj.si

2j. Step 3: SUMMARY.

UL | FRI

- OSINT on Oliver Zofič tells us that his wife has a hairdressing salon in Ljubljana.
- Shodan tells us that her website is located on Weebly in United States.
- You can sign up for an appointment over a web form.
- The personal data of EU citizens (names, email addresses, phone number…) is being stored on U.S. servers.
- Weebly fudges about this – their page says a lot about how they are going to ensure compliance but not yet. They advise you to put a notice on the web page about collecting data.
- There is no notice on janchy.si.
- This is a GDPR breach, making the owners personally responsible (up to 10 years in jail), and the business liable at 4% of their annual budget.

david.modic@fri.uni-lj.si

2j. Step 3: ATTACK VECTORS (PHYSICAL ACCESS)

UL | FRI

- Gain physical access to salon Janchy. Find an opportunity to insert a rubber ducky / malware package / keylogger into the system.
- One way to go about it would be to simply get a hair cutting appointment.
  - Get to the salon and say that you have a number of photos of what you wanted to look like on this here USB key.
  - Another solution would be to send phishing links in the comments section of the ”making an appointment” web form.
- The overall goal would be to gain access to Janja’s Mailbox.

david.modic@fri.uni-lj.si

2j. Step 3: ATTACK VECTORS (SOC ENG – petty cash)

UL | FRI

- Janja (we have her mail and business address) receives an email from the "information commissioners office".
- In it, "Andrej Tomšič" (an actual ICO deputy), tells her the ICO is about to start an investigation into the GDPR breach and outlines the reasons.
- Janja is told that she should immediately provide a privacy notice on her page and pay a fine, before she gets into real trouble.
- The fine is 500 EUR. It is not worth contesting this as any lawyer would charge more.
- The email contains a link to a "form" one needs to fill out. Drive by malware. PWNED.
- The email contains instructions on how to install a specific extension that "checks a webpage for GDPR compliance". It is actually an RDP trojan / keylogger. PWNED.
- The email contains instructions on how to pay the fine (the bank account is an online banking service, the money instantly transferred to Russia or China). PWNED.

2k. Step 3: ATTACK VECTORS (SOC ENG – blackmail)

UL | FRI

- Janja (we have her mail and business address) receives an email from an unknown source.
- In it, Janja is told how much she is on the hook for (jail time, large fines, etc. All true, by the way) if the ICO is notified.
- Now, she has a choice. Either *do nothing and get ruined*, OR *send a phishing email to her husband, Oliver*. If she tells anyone or Oliver doesn't open the email, the ICO gets notified about the breach.
- The email contains a payload, something like: emotet, formerly banking malware that analyses the targets inbox, learns their writing style and phishes on.

david.modic@fri.uni-lj.si

2k. Step 3: ATTACK VECTORS (SOC ENG – blackmail)

UL | FRI

- In previous steps we get access to someone's inbox. Either Janja's or Oliver's.
- We look at the emails, writing style, upcoming events, ongoing conversations…
- The interim goal is Oliver. The final destination is Barbara Domicelj.
- Depending on the information from step 2, we construct a phishing email that is mostly true (actual dates, correct names, documents that should actually require Barbara's approval…), but contains malware.
- If Oliver never, ever, writes to Barbara, we look through Oliver's mailbox and find someone who connects Oliver and Barbara. We exploit them.
- There are always ways to circumvent mechanical protection!

david.modic@fri.uni-lj.si

An IOT example

3a. Use of forensics to craft an attack

- MiSafes "smart" watch for children. Has a GPS and Bluetooth. Prevents calls from strangers, notifies parents when the child leaves a protected area (like school).
- Product with best intentions in mind. But a total *omnishables* of implementation.
- Consequence: A godsend to paedophiles everywhere.

david.modic@fri.uni-lj.si

3b. Use of forensics to craft an attack

- Through the use of a traffic analyser researchers (in Cambridge) find:
  - Communications are sent unencrypted.
  - The user records are not sandboxed.
  - Each user gets a sequential user id number.
  - The watch reports an id of the user. Unencrypted.
  - Commands are sent to the watch unencrypted with a prefix of the id.

david.modic@fri.uni-lj.si

3c. Use of forensics to craft an attack

- Consequences:
  - Researchers create a webapp which superimposes all users of MiSafes on **a local map with names of children and their photos tracking in real time**. It is like going to a candy store for child abusers. You can pick favourites!
  - Anyone can **turn on the MiSafes mic remotely and record conversations**.
  - Anyone can spoof any phone number to appear as if the call is coming from parents.
  - Anyone can remotely change the safe zone parameters, so that everywhere else is a safe zone (so no notification when child leaves, say, school).

david.modic@fri.uni-lj.si

An investigative example

Set the scene

UL | FRI

- As an example, I chose the Cambridge Analytica “scandal”, a well-known incident where Facebook indirectly interfered in the referendum on the UK's departure from the EU.
- It is not a classic attack, but it is a good illustration of a forensic investigation and the mistakes made by the University of Cambridge.
- I was one of the investigators, so I have first-hand experience with the case.
- Since it is concluded and the results of the inquiry public, I can talk about it.

david.modic@fri.uni-lj.si

Basic postulates

UL | FRI

- Few aspects to clear up before we start:
  - The moral aspect: Brexit as a result of the manipulation of the electorate.
  - Ethical aspect: Data were obtained without consent.
  - Legal aspect: breach of the GDPR and UK electoral law.
  - The University of Cambridge (CAM) couldn't care less about all of this.

UNIVERSITY OF CAMBRIDGE

david.modic@fri.uni-lj.si

Basic postulates …

UL | FRI

- The *only thing* Cambridge is interested in, is how the proceedings impact its reputation, and how to demonstrate that it has nothing to do with this.
- It is important to understand that in this case CAM is not seeking justice or moral satisfaction. All it wants is damage limitation.
- Sometimes this is the nature of our work.
- However. Sometimes things backfire *spectacularly*.

david.modic@fri.uni-lj.si

The first salvo...

- f
- lytica
- g that
- de).

So it starts…

UL | FRI

- The University is cheerfully oblivious, until the publication of the Guardian article.
- Cam is vaguely aware that their employee, Dr. Alexander Kogan, a Moldovan postdoc, wanted to do some sort of Facebook research.
- He applied for Ethics approval and was rejected.

david.modic@fri.uni-lj.si

The first reactions …

UL | FRI

UNIVERSITY OF CAMBRIDGE
Information Services

- CAM statements to the public (and employees):
  - *Kogan has a home life, and has hobbies* [for example illegally gathering data ☺].
  - *If he was not abusing CAM assets while indulging in his hobbies, then this is none of our business. And stop* pestering *us.*
- Employees are told that they can comment, BUT not on the behalf of the University (this is SOP in any case).
- Kieren is told by the CISO that this is a storm in a teacup and that he should take it easy. "*It will all be over in a day or so*".

david.modic@fri.uni-lj.si

A few days after the Guardian article …

BBC RADIO CAMBRIDGESHIRE

- … Kogan is hosted by the BBC Radio 4. Kieren listens to him on his way to work. *This is not a verbatim transcript.*
- **Kogan**: *I did not directly collect all the data through the application* Your digital life. *I only got the direct data from its users. … To be clear, they agreed with processing their data, and the data of all their Facebook friends.*
- **host**: *Was this informed consent, and did they know what permissions they gave you?*
- **Kogan**: *They ticked a box in an online form, and it was clearly stated* in the small print *what type of access they are giving me.*

In case you missed it:

Kogan -> collects data from the users of his fb application.

Users -> consent to the processing of their **AND** their *friends'* data.

david.modic@fri.uni-lj.si

A few days after the Guardian article II.

BBC RADIO CAMBRIDGESHIRE

- **host**: *But could the users of your app access the results of the tests they took without this consent?*
- **Kogan**: *Of course they could! Every third Thursday of the month between 23:58 and 00:02, they would need to submit a video of a ritualistic slaughter of their pet budgie, and submit the recording to an undisclosed e-mail address. They had this option, but it seems that none of the respondents chose it, for some reason. Everyone preferred to tick the privacy invasion box. Which, of course, is not what we call it, ha ha.*

In case you missed it:

I am paraphrasing here, but in a nutshell, people were led to believe that they would only access the analysis of the tests they took, if they ticked a box. The implications were not clear.

david.modic@fri.uni-lj.si

A few days after the Guardian article III.

BBC RADIO CAMBRIDGESHIRE

- **host**: *Haha… Did you use any Cambridge University services or equipment in your research?*
- **Kogan**: *No way! That would be a blatant violation of research ethics. I did everything through my own company Global Science Research* [GSR]. *The University of Cambridge and GSR are two completely separate legal entities.*
- ***host***: *I see. How did you conduct data collection?*
- **Kogan**: *I used Qualtrics.*

- Kieren develops a nervous tick at that moment.

david.modic@fri.uni-lj.si

At the UIS

UL | FRI

- **Kieren** talks to the sys admin: "*Do we have a Qualtrics license?*"
- **Sys Admin**: *We do.*
- **Kieren**: *Does Kogan have a user account?*
- **Sys Admin**: *Yep.*
- **Kieren**: *Can we access his data collections?*
- **Sys Admin**: *That would be an invasion of privacy, but I can list the names of the files and associated surveys. For example this one: Facebook personality data.*

UNIVERSITY OF CAMBRIDGE
Information Services

david.modic@fri.uni-lj.si

Before we discuss further

UL | FRI

- (Quiz) What do you think Kieren should do now?
  - Look at file servers for the whole Uni and for the School of Psychology.
  - Check Kogan's work resources and cloud resources connected to work.
  - Check all connections between Cantab and Kogan
  - Look at Kogan's work email (*by the way work emails do not enjoy any kind of privacy protection. Just so you know. Do not use work accounts to plan robbing banks or dating someone on the side).*
  - Look at access logs…
  - … and talk to everyone who might reasonably have access to the data.

david.modic@fri.uni-lj.si

Before we discuss further

UL | FRI

- (Quiz) Is it a problem for a University to breach privacy laws?
  - Well, yeah. They are not exempt from the law.
- (Quiz) What worries Cambridge here?
  - For them, this is a public image issue. They have connections aplenty with various committees and MP's. They are not bothered about the law at all. They believe they can squash anything. They only thing is the damage to the reputation of the University and a (slight) decrease of popularity.

david.modic@fri.uni-lj.si

Investigation starts

UL | FRI

- Kieren is now almost sure that Kogan used the infrastructure of the University for his research.
- Kieren looks at the Cambridge shared file space and finds facebook_personality.iso file.
- The file contains non-anonymized data (demographics, likes, metadata, personality tests in some cases, and more) of 30+ million Facebook users.
- For a lark, Kieren, he looks for himself and me in the file and finds us both.
- The ISO contains the data and browsing and indexing script.
- Kogan did not write this script, a developer did.

david.modic@fri.uni-lj.si

Finding the script developer

UL | FRI

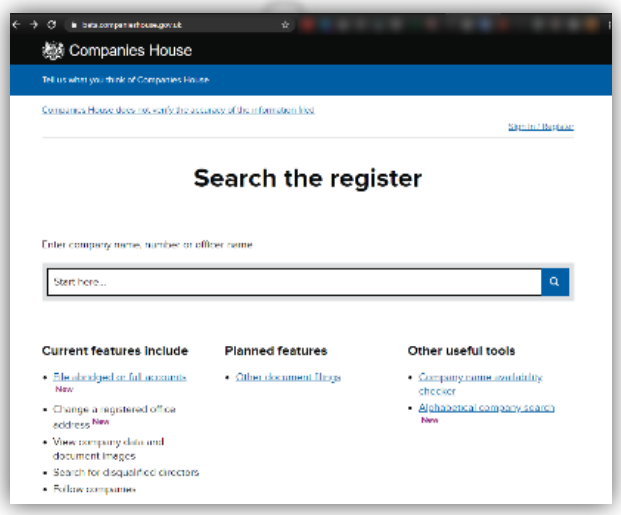
- Kieren asks around who helped write the database search engine (literally sends an email).
- A colleague responds. It turns out that he and Kogan were both contacted by CA and offered £1M for the data.
- The colleague refused to cooperate ("*I don't need the money if the price is my integrity...*"). He is unaware how Kogan responded.
- He does recall that Kogan founded the company Global Science Research projects [GSR] the day after they were contacted by CA.

david.modic@fri.uni-lj.si

GSR

UL | FRI

- A visit to the English Companies registry shows that GSR is based in a property owned by the University of Cambridge.
- This record has now been deleted.
- The company no longer exists either.



david.modic@fri.uni-lj.si

What do we know so far …

UL | FRI

- Kogan is employed by the University of Cambridge.
- Kogan collects the data of 30M facebook users in an illegal and unethical way.
- Kogan founds Global Science Research projects (GSR).
- GSR sells facebook data to CA £1m.
- CA analyzes the data and sells it along with the analysis to the Vote Leave organization (Brexit lobbyists).
- With the help of CA, Vote Leave influences the results of the referendum on the exit of the UK from the EU (52:48 for exit).

david.modic@fri.uni-lj.si

A short intermezzo

UL | FRI

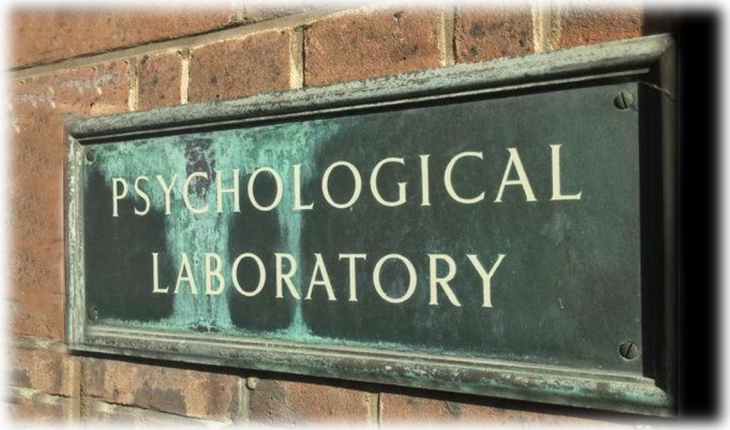
- (Quiz) How does Vote Leave influence voters with CA's help? Do they extort them: "*We have information that you like to wear mismatching socks! We will publish this if you do not vote for Brexit?*"
  - No.
- (Quiz) What do you think they actually did? And how do you think an effective behavior change campaign works? (in this case, this is clearly the same question ☺).
  - Target-focused, but appears general.
  - News that appear general, but target only some individuals.
  - Appear to be coming from legitimate sources.
  - The goal is not to change behavior with a single transaction, but to shape it slowly, day by day.

david.modic@fri.uni-lj.si

School of Psychology (Kogan's workplace)

UL | FRI

- The Psychology Department invites CamCERT to inspect their servers (or at least the 9 of them that Kogan could access). They want to clearly demonstrate, that they were not complicit.
- The servers truly are completely empty. Completely. Bonus question: *How many servers without an operating system do you have running in your server room, and why?*
- But, in the lobby of the department, there is a dumb terminal that connects to a single endpoint through an encrypted tunnel.
- Access is protected with two passwords.
- There is no receptionist at the Department of Psychology.
- Any random passerby can access the terminal unsupervised.



david.modic@fri.uni-lj.si

The terminal at the Psychology Department

UL | FRI

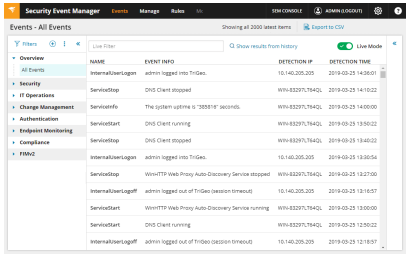
- Two complex passwords represent a huge, almost insurmountable, obstacle.
- Except when they are written on a *post-it* note on the table under the keyboard (what is love and baby dont hurt me).
- Kieren logs in and finds a single file on the remote server: facebook_personality.iso.
- It is the same ISO he already looked at. The hash is the same.
- The terminal tunnels to a CA server, where this iso is located.
- The terminal is also attempting to connect to a google drive account, but the connection is blocked.

david.modic@fri.uni-lj.si

The terminal cont'd

UL | FRI

- Anyone who can enter the Department of Psychology, has access to the personal data of Facebook users. Which means *anyone* physically present.
- The University's award winning security policy[tm] only tracks and logs unsuccessful access attempts.
- Which means that anyone with a password found under the keyboard, can access the terminal without digital forensic traces.
- A check of netflow logs shows that the terminal in question is trying to connect to a google drive linked to Alexander Kogan's gmail.
- So, even better, you did not even need physical access to the machine. Only the link to the file on Alexander's gdrive.

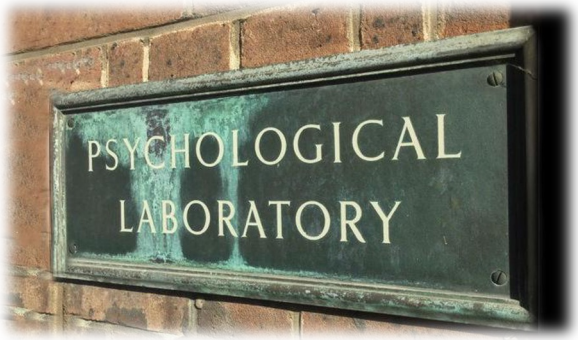


david.modic@fri.uni-lj.si

School of Psychology (students)

UL | FRI

- Kieren walks around the Psychology Department. He asks whether Kogan had any doctoral students.
- He had four. Kieren asks to see their computers.
- All four are empty.
- Two have full trash cans. There is a facebook_personality.iso file in both.
- It is now clear to both of us that the University is involved up to its neck.
- Kogan's students are actively obstructing the police investigation and destroying evidence.
- I do understand students. If the mentor assured them that there was nothing wrong with the data, then they did not doubt him.
- However, when the investigation started, they should have come forward. Because now they are accomplices and have destroyed evidence in an active investigation.



david.modic@fri.uni-lj.si

What do we know so far?

UL | FRI

- The University provided software, server space, real estate, and human resources (students) to illegally acquire, store, and process data that Kogan subsequently sold to CA.
- Data was not stored according to GDPR.
- The data were not obtained ethically.
- Part of the sold IP was stolen (e.g. software was not paid for).
- Most of the owners of the data did not give their consent for the processing, sale and storage of their personal info.
- However, the University still believes this is not its problem.
- They additionally are engaged in active destruction of evidence (deleting Kogan's e-mails).

david.modic@fri.uni-lj.si

Consequences

UL | FRI

- The police contact the University and request an informative interview.
- The CISO rejects it despite (our) advice to the contrary.
- The CISO is not concerned because the Information Commissioner (who is leading the investigation) is full of Cambridge graduates ensuring that things will keep quiet.
- And if that does not work, Cambridge will simply fire someone.

david.modic@fri.uni-lj.si

Kieren now calculates

UL | FRI

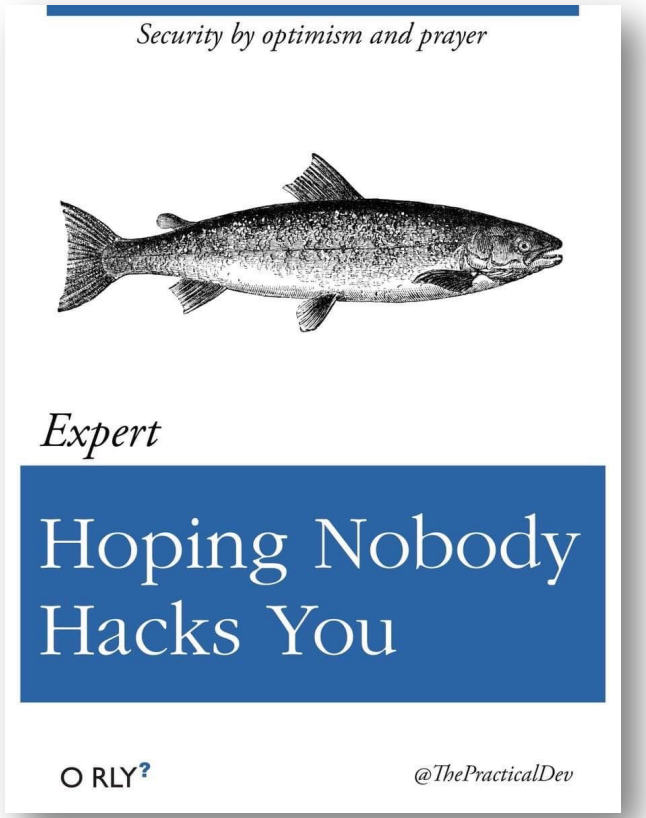
- At this point, Kieren knows his job is on the line.
- He will be charged with impeding the investigation and the destruction of evidence, as well as obstruction.
- He was following instructions and objecting to them constantly, but no one will care.
- He is the third in line to the throne (and I am the fourth ☺). But the first two are untouchable (One just arrived to post, and the other is non-caucasian and has a disability).
- Kieren finds himself another job out of the Country and quits.
- Then he whistleblows to the ICO.
- The CISO is angry, but not bothered (nothing will come of this scandal, he thinks, because he has friends in the ICO's office).

david.modic@fri.uni-lj.si

Kieren now calculates

UL | FRI

- ICO hires an Australian lawyer to lead the investigation.
- Even on the eve of the publication of the report, Cambridge thinks they will remain untouched.
- Little do they know that the ICO report that will shake them thoroughly is only the first incident…
- Immediately after this incident comes the second, even worse one (the manipulated American elections).
- The result of the investigation of the second incident is a 10 Million GBP fine and constant external audit of the University's data.
- Which means, among other things, the loss of defense projects worth hundreds of millions.



david.modic@fri.uni-lj.si

Summary

UL | FRI

- It is not news that forensics are used in INFOSEC.
- I have given you just a few examples on how the tools used by white hats are also used by blackhats.
- My focus is on human attack vectors, but forensics are very helpful in that too.

david.modic@fri.uni-lj.si

FRI
UNIVERZA V L]UBL]ANI
Fakulteta za računalništvo in informatiko

Univerza *v Ljubljani*
Fakulteta *za računalništvo in informatiko*

Questions?

(we are not done yet ☺)

www.fri.uni-lj.si

www.facebook.com/ulfri