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

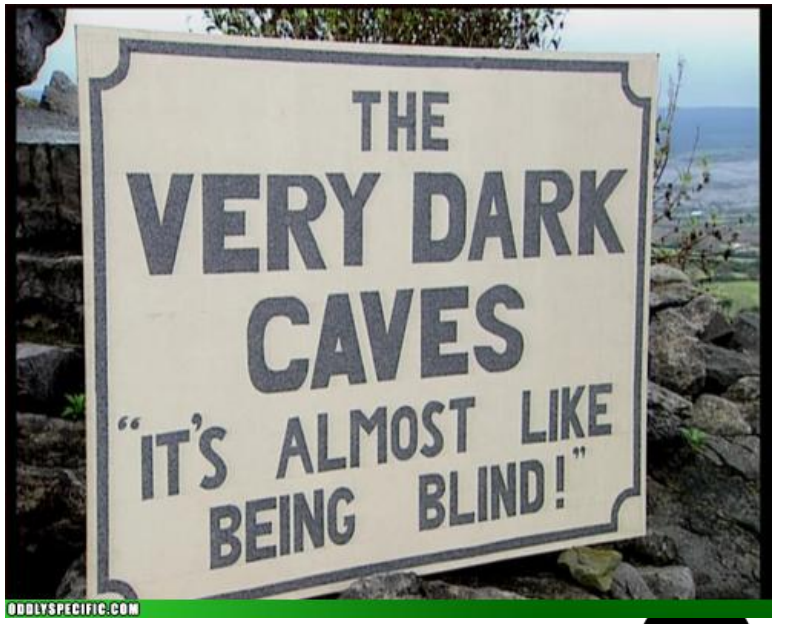
OSINT

dr. David Modic

04/11/20

Homework 2 comments

- You all did as requested. There were some growing pains, which were mostly my fault.
- The purpose was for you to familiarize yourselves with the tool.
- As a suggestion, I would try different queries if I was you, just to see how it works.
- Most of you did not use parts of your emails etc. This did not impact your grade.
- It is useful, though, to try a few things, like in my case: *david, david.modic, modic, modic.david, exeter.ac.uk, ex.ac.uk, cl.cam.ac.uk…*
- **Well done, though!**



david.modic@fri.uni-lj.si

The story so far…

- We learned about Ethics in penetration testing.
- We learned about the process of penetration testing – the phases, the gotchas and the general outline.
- We explored the breach database and connected to a Kali VM.
- Today we will talk about Open Source INTelligence (OSINT) gathering.

Outline of the talk

- A few definitions
- The process
- Practical examples
- Homework

Terminology

- We stole the terminology from NATO.
- Or vice versa? Does not matter.
- Many of the terms are defined in the *NATO Open Source Intelligence Handbook* (now declassified, initially written by my colleague Kieren Lovell).
  - https://goo.gl/3E8ZNR (QR is here ->)
  - Also on moodle.

Intelligence

- (Quiz) What is SIGINT?
  - SIGnals INTelligence. What does that mean?
  - Information that is gathered from interception of Signals.
- (Quiz) What kind of intelligence signals are there?
  -
    -
  -
    -

Intelligence

- (Quiz) What is SIGINT?
  - SIGnals INTelligence. What does that mean?
  - Information that is gathered from interception of Signals.
- (Quiz) What kind of intelligence signals are there?
  - COMINT. What does it mean?
    -
    -
    -

Intelligence

- (Quiz) What is SIGINT?
  - SIGnals INTelligence. What does that mean?
  - Information that is gathered from interception of Signals.
- (Quiz) What kind of intelligence signals are there?
  - COMINT. What does it mean?
    - COMmunications INTelligence, that is, analysis of communication between people (emails, phone, face 2 face, forums, etc).
  - ELINT. What does it mean?
    -

Intelligence

- (Quiz) What is SIGINT?
  - SIGnals INTelligence. What does that mean?
  - Information that is gathered from interception of Signals.
- (Quiz) What kind of intelligence signals are there?
  - COMINT. What does it mean?
    - COMmunications INTelligence, that is, analysis of communication between people (emails, phone, face 2 face, forums, etc).
  - ELINT. What does it mean?
    - ELectronic INTelligence, that is the analysis of electronic signals not used in communication directly (protocols, metadata in various contexts, etc).

Intelligence signals continued…

- (Quiz) What kind of intelligence signals are there?
  - HUMINT. What does it mean?
    -
  -
    -
  -
    -
  -
    -

Intelligence signals continued…

- (Quiz) What kind of intelligence signals are there?
  - HUMINT. What does it mean?
    - HUMan INTelligence, that is, information gathered from interpersonal contact and provided by human sources.
  - IMINT. What does it mean?
    -
    -
    -
    -

Intelligence signals continued…

- (Quiz) What kind of intelligence signals are there?
  - HUMINT. What does it mean?
    - HUMan INTelligence, that is, information gathered from interpersonal contact and provided by human sources.
  - IMINT. What does it mean?
    - IMagery INTelligence – analysis of pictures – photographs, satellite imagery etc.
  - MASINT. What does it mean?
    -

Intelligence signals continued…

- (Quiz) What kind of intelligence signals are there?
  - HUMINT. What does it mean?
    - HUMan INTelligence, that is, information gathered from interpersonal contact and provided by human sources.
  - IMINT. What does it mean?
    - IMagery INTelligence – analysis of pictures – photographs, satellite imagery etc.
  - MASINT. What does it mean?
    - Measurement And Signature INTelligence – detection and analysis of signatures of specific targets (e.g. finding out where a server room is because of an increased power draw, or finding where a secret operation is taking place because of heavy biometric security required to enter a drycleaners ☺).
  - GEOINT and others. Of course there is also OSINT!

Intelligence (OSINT)

- (Quiz) What is OSINT?
  -
  -
-
  -
-

Intelligence (OSINT)

- (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?
  -
-

Intelligence (OSINT)

- (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'.

Basic security terms – Threat Model

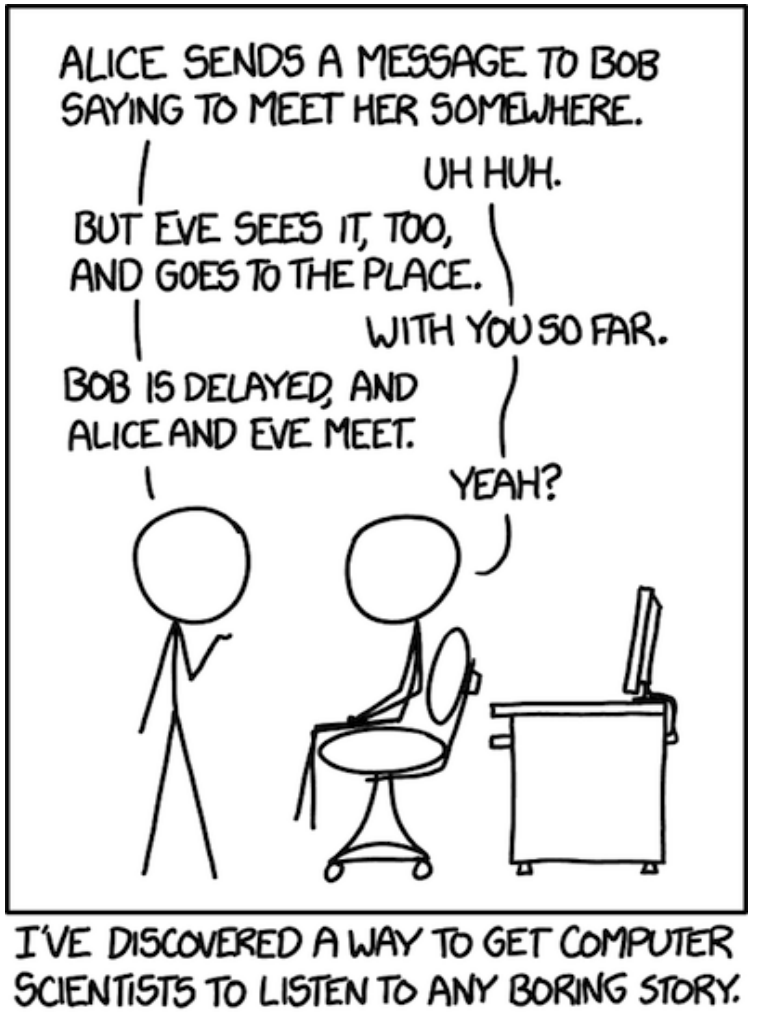
- (Quiz) What is a Threat Model?
  -
  -
  -

Basic security terms – Threat Model

- (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.

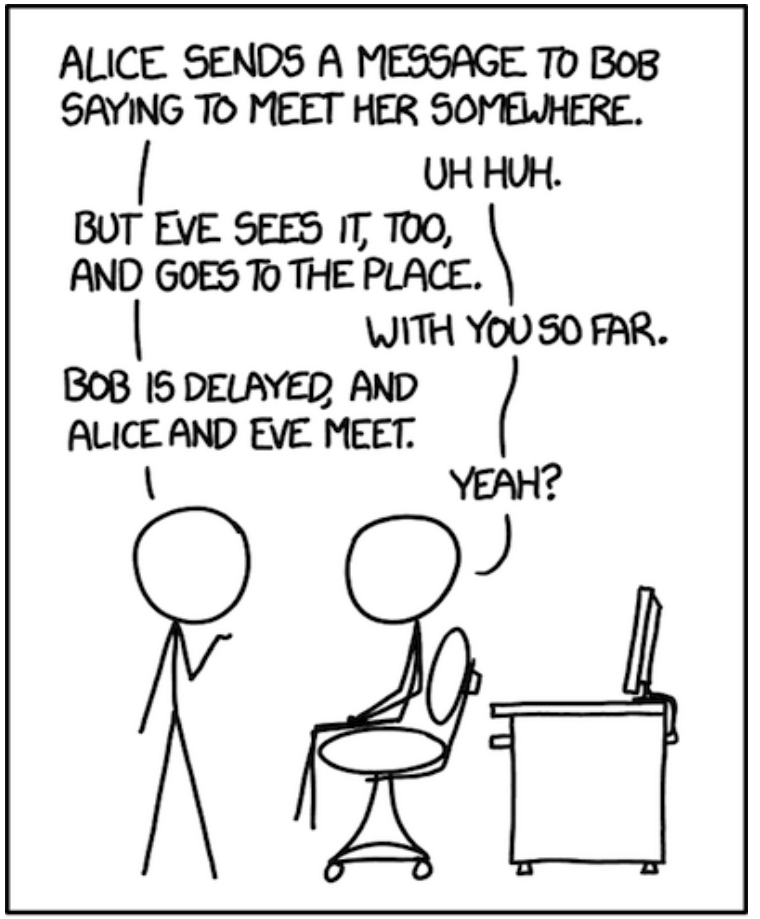
Basic security terms – actor names

- (Quiz) What generalized names do we use in threat modelling?
  -
  -
  -
  -



Basic security terms – actor names

- (Quiz) What generalized names do we use in threat modelling?
  - Alice, Bob, Carol, Craig (generic),
  - Eve (eavesdropper)
  - Mallory (malicious attacker),
  - Trudy (intruder)…



Basic security terms – Attack vector

- (Quiz) What is an Attack Vector?
  -
  -
  -
-
  -

Basic security terms – Attack vector

- (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?
  -

Basic security terms – Attack vector

- (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).

What does NATO say about OSINT?

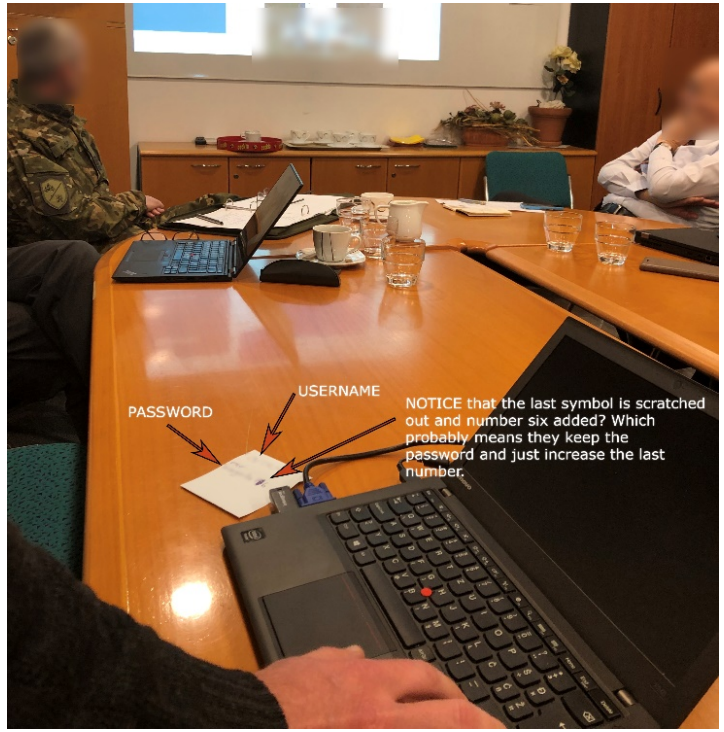
" OSINT was fairly new to us and once the term was understood we placed a signals intelligence analyst in charge of OSINT. At the tactical level, it seemed to be effective after the fact. There were three successful attacks against coalition forces aircraft in a specific area. We couldn't figure out the "how" and 5Ws [who, what, when, where, why] but our OSINT analyst found a downed aircraft video on the Internet that helped us identify the ingress and egress routes used during the attack that led to a "no fly" area and successful area denial missions in our area of operation. "

All-Source Operation Iraqi Freedom 2008-2009, Intelligence Analyst, Combat Aviation Brigade

david.modic@fri.uni-lj.si

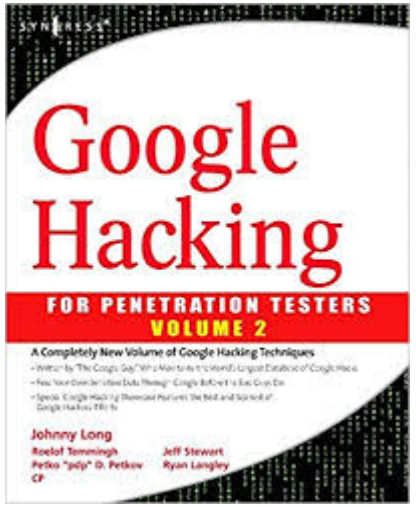
What does NATO say about OSINT (in a Nutshell?)

- *There is, if anything, too much information to process.*
- *Information is unreliable.*
- *Operations security (OPSEC) is hard. Which works for you, but also against you.*
- *There is still the question of copyright and IP.*



Typical tools used in OSINT

- *Shodan.io* – this is in the next lecture.
- *nmap and breach databases* – this was in the previous lecture.
- *Google hacking* – what is says on the tin. Next slide – more details.
- Agregator tools like *spiderfoot*.

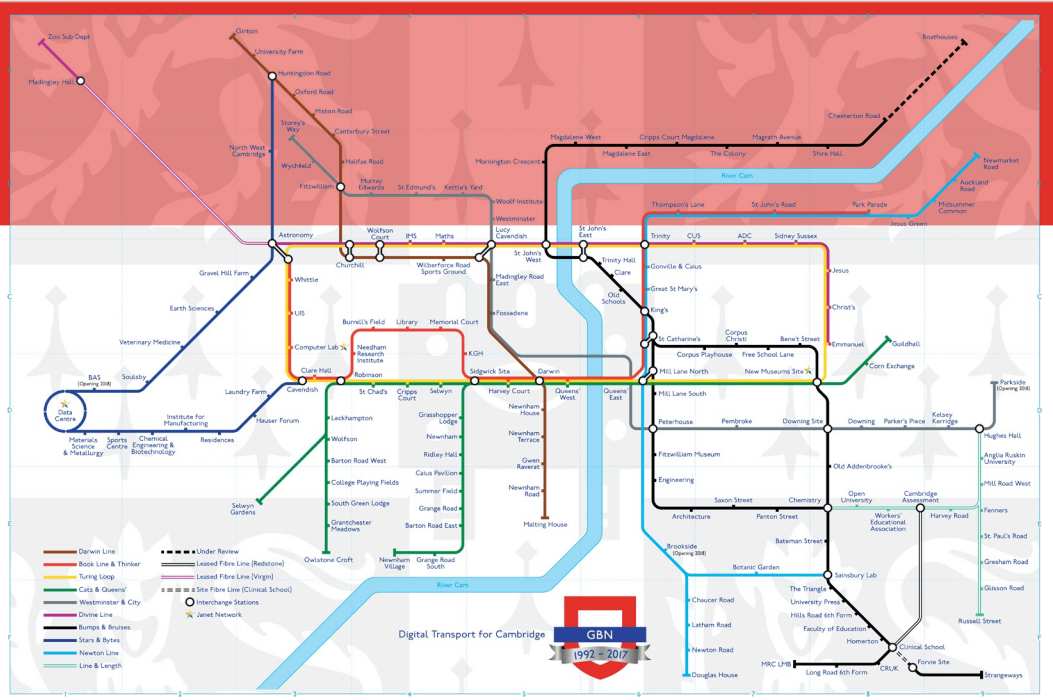


Using human attack vectors

- Why should we focus on human attack vectors?
  - Because we are all shit at the technical aspects of CS and so we deal with people?
  - Because there is good evidence that they are effective?
  - Because, traditionally, comparably less money and effort is spent on user education (compared to license fees and infrastructure)?
  - Because human attack vectors are fun and mechanical attacks are boring?
  - …

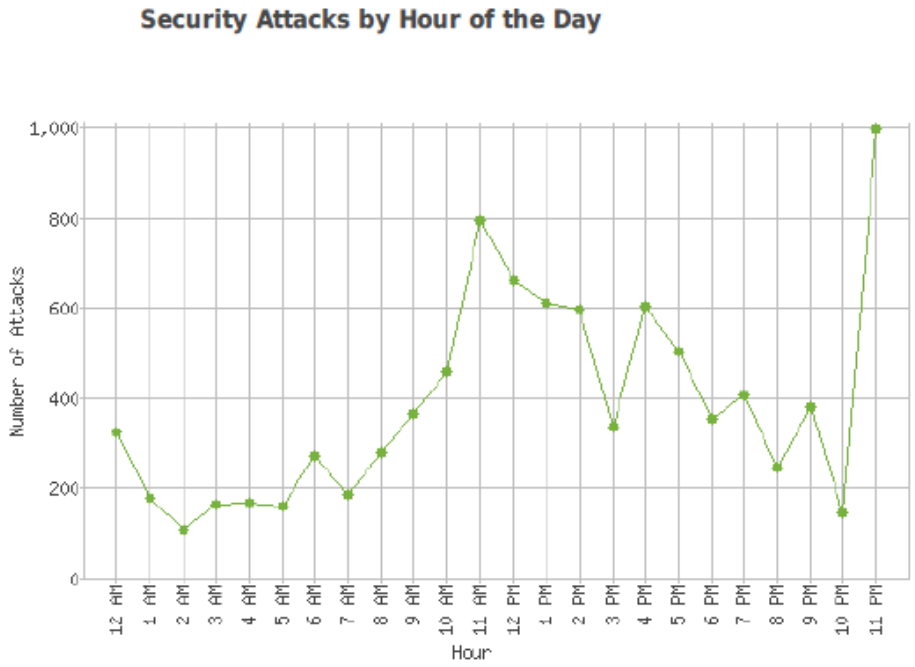
To set the scene

- Cambridge University:
  - ~ 12.000 employees (approx. 8.000 academics)
  - ~ 21.000 students
  - Geographical footprint – literally from Pole to Pole ☺.
  - Richer than some Countries.
  - >250.000 active IP assignments + NAT. No one knows how many devices.
  - The biggest local private network in Europe.



Security arrangements

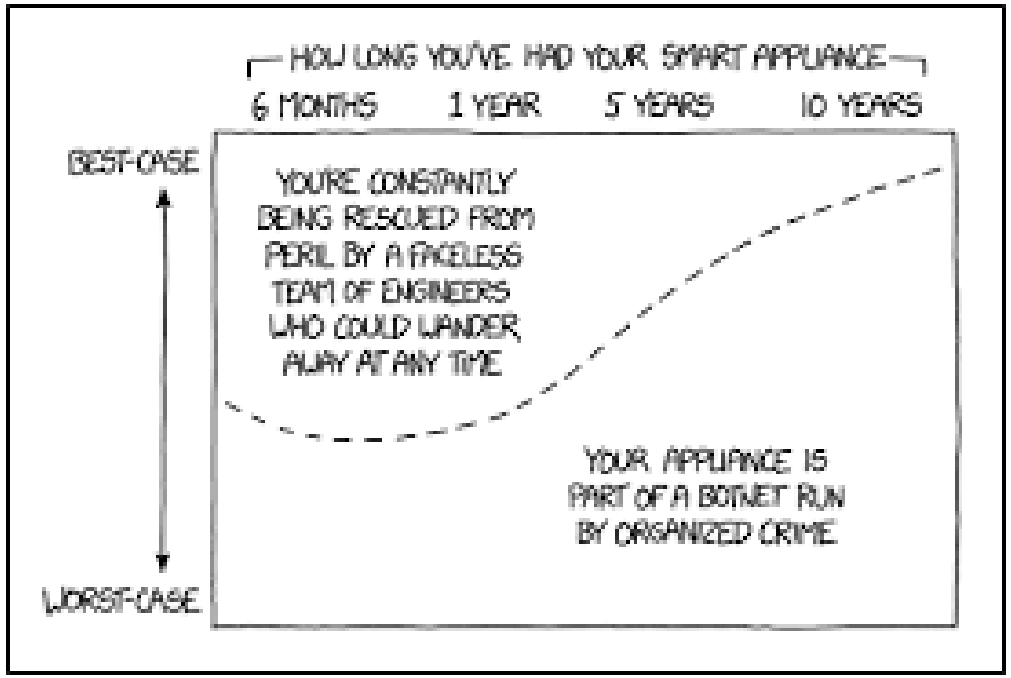
- Most of the traffic is routed through two CISCO Firepowers.
- IDS daily reports.
- As an example a typical month some time ago.
- 9.278 detected intrusion attempts (DDOS – 4.921, WordPress – 1.135, Malware – 837…).
- Targeted domains – www.cam.ac.uk , app.admin.cam.ac.uk , mail13.admin.cam.ac.uk



david.modic@fri.uni-lj.si

Threat modelling

- ~ 200.000 detected attacks monthly.
- ~ 1.700 incident reports.
- **> 99% use human attack vectors.**
  - Malware
  - Phishing
  - Identity theft and intellectual property of the University.



- Most attacks originate from China, Russia, N. Korea…
- Frequencies sharply increase when facing extraordinary events (e.g. before Brexit referendum, before GE 2017, etc).
- People are clearly an important attack vector.

A short break

- Let's take 10 minutes and then move on to practical examples. Agreed?

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

OSINT - EXAMPLES

doc. dr. David Modic

21/03/19

Exercise Mercury

- From a CTF hackathon between TalTech, Estonia and Cambridge.
- Report is on *ucilnica*, classified as confidential, [now internal], do not disseminate.
- One week. Open source intelligence gathering, and passive attacks. Any detection losses points. No active exploits. Emphasis on social engineering. We started the event with a lecture on psychology of security.
- We will do the whole lecture later on in the course. But here is a summary.

Summary of psychology of security

- Exploiting people is cheaper, easier, and requires less prior knowledge.
- There are psychological mechanisms that make it likely to ensure compliance. Article about that is on ucilnica.
- It is safe to assume: Individuals will not be familiar with the company‘s security policy (unless they wrote it), very little authenticity checking, differences between fake and real communication will be negligible, it pays to introduce time pressure and cognitive load.
- We do not have the time to go into more details here.

Framing

- After the talk, teams were formed. Let's call one of them **TT** (Team Talinn). Cambridge attacks TalTech, TalTech attacks Cambridge.
- TalTech destroys Cambridge. Cambridge would inconvenience TalTech, they would have destroyed our network completely.
- They found, amongst other things, that about 50% of apache web servers were unpatched, a number of SQL injects, a way to *telnet* into the main router of the University, etc. It is all in the Exercise Mercury report.

Reaction of management


CRIME BEAT

DUI FAIL

A man arrested for DUI on July 31 told a cop the stop sign turned red too fast for him to stop.

- Cambridge management is *unhappy* (reputation effects, narcissism takes a beating).
- We point out to them that:
  - (a) we had 30 people to PEN test us for free for a week, saving at least a million pounds, and
  - (b) if we won, nobody would want to play with us again. But now, there are plenty of Institutions who are looking to show Cambridge how crap we are, compared to them.
- Also, we already fixed everything that was discovered ☺.
- Here is one example of what **TT** did.

Picking the target

- TT is offered three names. One of them is the Cambridge CISO. Let‘s name him **Lawrence B** (fake name, to be clear. And yes, I know you can all use Google).
- TT looks at the internal directory of the Uni, but believe they need to sign in to access it. But do they?
-
-

P

-

-

to

-

-

Picking the target

- TT is offered three names. One of them is the Cambridge CISO. Let‘s name him **Lawrence B** (fake name, to be clear. And yes, I know you can all use Google).
- TT looks at the internal directory of the Uni, but believe they need to sign in to access it. But do they?
- They look at the UIS Deputy director. They find his username: sr745 .
-

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Picking th

- TT is offe
  him **Lawr**
  Google).
- TT looks a
  access it.
- They look
-

‘s name

l use

› sign in to

.

Home | About | Get started | News | Events | Cyber security | Initiatives | A-Z | IT Service

University Information Services

About

How we are structured

How we work with you

Our people

- Dr Sibel Allinson
- Dr Jenny Barna
- Dr Clare Bartlet
- Kevin Brown
- Dr Paul Calleja
- Dr Ruth Charles
- Andrew Cox
- Chris Edwards
- Dawn Edwards
- Dr Mark Ferrar
- Mark Galvin
- Monica Gonzales
- James Hargrave

Steve Riley, O.B.E.

Deputy Director, Service Operations

Contact Steve

- Lookup
- vcard

About Steve

Steve was Interim Director General for Information Technology at the Departmer
2015, where he had responsibility for the day-to-day running of the Department
citizens, as well as modernising services for hosting, networking, end user compu

https://www.lookup.cam.ac.uk/person/crsid/sr745/vcard

Picking the target

- TT is offered three names. One of them is the Cambridge CISO. Let‘s name him **Lawrence B** (fake name, to be clear. And yes, I know you can all use Google).
- TT looks at the internal directory of the Uni, but believe they need to sign in to access it. But do they?
- They look at the UIS Deputy director. They find his username: sr745 .
- Therefore Lawrence B‘s username should be: lb[NNN], and his email: lb[NNN]@cam.ac.uk.

OSINT continued…

- Lawrence is cautious. TT finds his page, but the CRsID leads to a student.
- However, Steve Riley and Lawrence both work in the same Department (UIS).
- Steve's email addresses are sr745@cam.ac.uk and steve.riley@uis.cam.ac.uk AHA!
- Lawrence Bozic is thus **lawrence.bozic@uis.cam.ac.uk**?
- TT sends an email to *ssafgfcfgs@uis.cam.ac.uk*. Gets a delivery fail notice.
- Then, they send an email to lawrence.bozic@uis.cam.ac.uk and the email does not bounce.
- They call the UIS helpdesk and ask them to check whether the spam filter has intercepted the mail. Helpdesk confirms, TT asks to be taken off the spam list, and the email goes through to Lawrence.

More prep

- TT visits LB's web page. Lawrence writes (emphasis mine):

"His earlier experience includes architecting and building a managed cyber security service for the consulting firm Deloitte, and designing and then delivering technical security operations and incident management"

- TT decides that Lawrence needs to be invited to a fake conference in Tartu, Estonia.
-

More prep

- TT vi… …s (en…

"Hi… …d bu… …the consu… …deli… …ident …ageme…

- TT d… …vited… …nia[].
-

FAKE

Genuine

More prep

- TT visits LB's web page. Lawrence writes (emphasis mine):

"His earlier experience includes architecting and building a managed cyber security service for the consulting firm Deloitte, and designing and then delivering technical security operations and incident management"

- TT decides that Lawrence needs to be invited to a fake conference in Tartu, Estonia.
- They send him an invite.

Writing reports

Dear [redacted]

On behalf of University of Tartu and Skype, we would like to request the pleasure of your company to be a perspective keynote at the **Education in Cybersecurity: Digital Engineering and Architecture Conference** at Tartu University on 10 April 2018. Since we find your experience to be the best fit to the conference agenda, your participation would be **fully funded** from our side (accommodation, tickets, daily expenses) in the case if you are willing to come.
Hereby I would like to share more information and details about the conference.
You may have a look at the agenda at our website.
https://eddea.org
You also may fill in the registration blank for speakers. Please, kindly specify that you were invited by Saber Yari.

Thank you for your time and consideration.

Kind regards,
Saber Yari
Senior Project Manager
Education in Cybersecurity: Digital Engineering and Architecture Conference

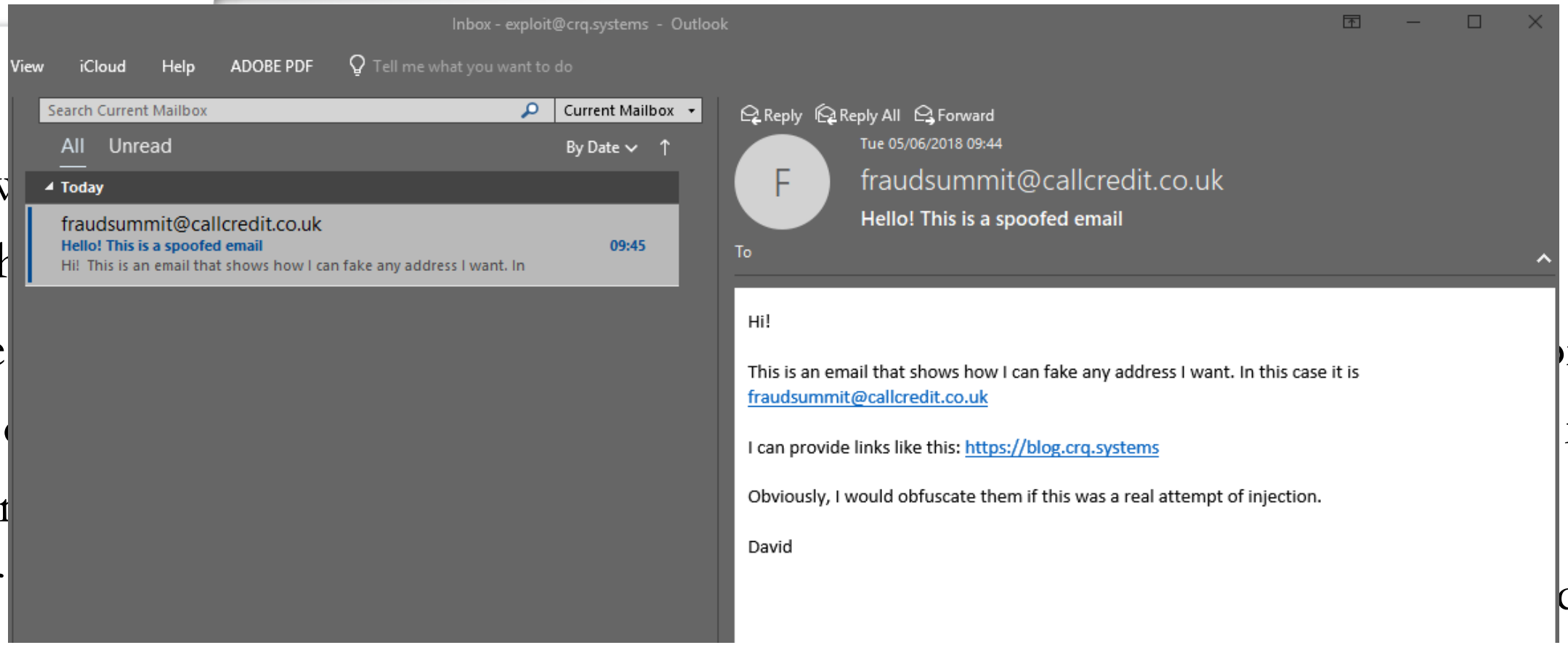
- The email refers to Lawrence's interests - digital architecture and security (see his vanity page).
- It strokes his ego (*You are so cool, the best choice really, we'll pay for everything*).
- The actual conference exists, but the fake URL is subtly different.
- Mail is sent at 16:05.
- Link leads to a click-through server and then redirects to a *sloow* loading fake conference page.
- Saber Yari exists.

The email

- Lawrence should have noticed that the email did not arrive from Saber Yari, right?
- We all know how easy it is to spoof an email address. The example here is from an organizer of a security conference (held at the Royal Society of Engineers in London).
-

The

- Lav
  righ
- We
  an
  Lor
- Of



om

in

do

it in real life? Not many. And the CISO did not either.

The email

- Lawrence should have noticed that the email did not arrive from Saber Yari, right?
- We all know how easy it is to spoof an email address. The example here is from an organizer of a security conference (held at the Royal Society of Engineers in London).
- Of course, Lawrence could have checked the headers. But how many people do it in real life? Not many. And the CISO did not either.

What happens?

- Lawrence loses patience, because the link from his desktop is *so slow*.
- So he also clicks from **his laptop**, and **his mobile phone**.
- The result: 3 of the CISO‘s devices would be compromised.
- TT does not stop there, though.
- They could have installed a C&C client on L‘s devices.
- But they expect our IDS detects outgoing C&C traffic, and blocks it.
- It doesn‘t, but they don‘t know that (*academic freedom FTW. Why did we pay £2M for an IDS if we don‘t use it?*).

What happens?

- TT spoofs Lawrence's email address…
- …and sends another email to the UIS helpdesk.
- „Lawrence" asks the helpdesk to whitelist his desktop machine and stop monitoring it, because he is *doing science* on it.
- Helpdesk obeys (*Kieren stands behind them and immediately reinstates monitoring*).
- And now TT would have **full unmonitored access** to the CISO's machine(s).

Fallout from the exercise

- Lawrence *knew* he was a target. We also told him when (roughly), and who will be attacking.
- Lawrence is *quite* upset. He says that this is *unfair* and that he does not have admin access anyway, so he is not an optimal target.
- We gave him two scenarios:

MODEL 01 MODEL 02

Fall

- Lav
  be
- Lav
  adr
- We

SCENARIO 1 „…not *yet* have admin access“:

- „Lawrence“ writes to sys admin and requests server room access for himself, or for a fellow academic.
- The admin enables access. No reason not to.
- “Lawrence”’could also have a UNI card made, by the way. In-house.
- Somebody shows up with a raspberry Pi and a usb stick. Game over.
- **Result – whole network monitored by someone else. The Pi filters traffic and does MITM when needed.**

ill

MODEL 01 MODEL 02

david.modic@fri.uni-lj.si

Fallout fr

- Lawrence
  be attacki
- Lawrence
  admin acc
- We gave h

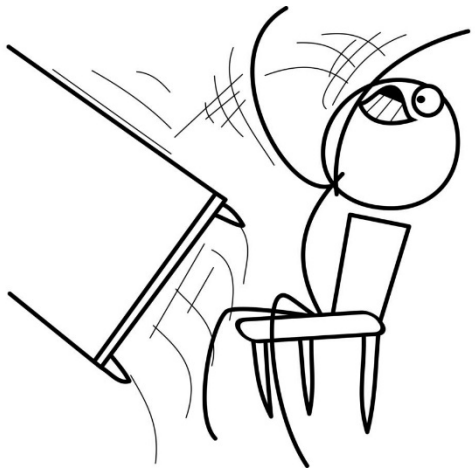
ill

SCENARIO 02 „Too unimportant “:

- „Lawrence“ writes an email to the university Registrar (In charge of staff and degrees amongst other things).
- The email says: „Please look at this spreadsheet that contains our latest risk analysis vis-a-vis new threat landscape.“
- There is an Excel file attached, containing a rootkit.
- The Registrar is definitively interested in finding out about new threats. And the email is from a *trusted source*.
- **Result – exploiting someone „unimportant“ leads to getting to someone who has access to academic records of all staff and students. Anyone fancy a PhD from Cambridge?**

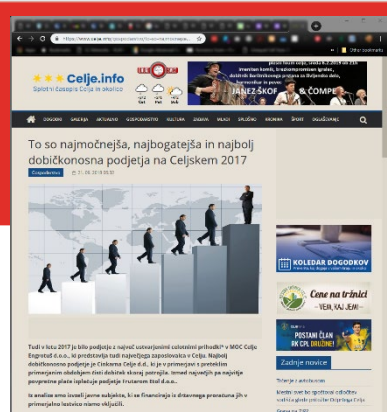
Summary / take-home messages

- Technical security is a pre-requisite!
  - (remember: > 9000 attempts/day. Most caught by the IDS. No IDS => 9k incidents/day).
- But ... mechanical safety is not enough!
  - Example given bypasses technical solutions.
- No one is unimportant enough.
  - Everyone has access to someone higher up.
- Understanding security psychology yields results.
  - TT used several points I made in the lecture to a great effect.
- Knowing you are a target does not help (or hinder).
  - Realistically, we are all targeted constantly, and this does not seem to have an impact on our behaviour.



Another OSINT example (from recent FRI open days)

- The focus was the region of Celje (that is where the pupils were from).
- Only OSINT, passive attack(s). Nothing illegal.
- I will suggest further actions, but not do them. By this point in the course, you know why ☺.



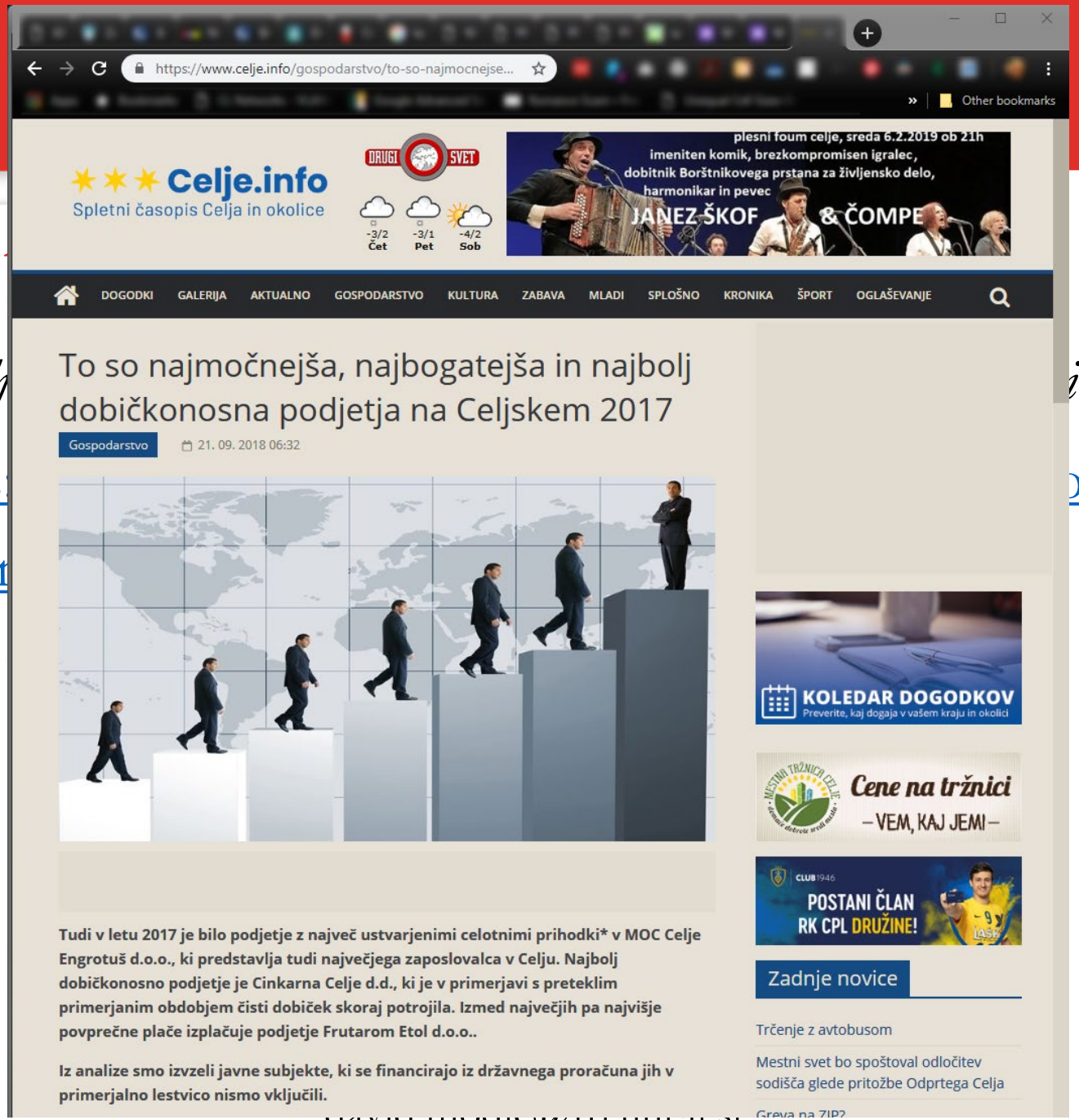
1. Picking the target

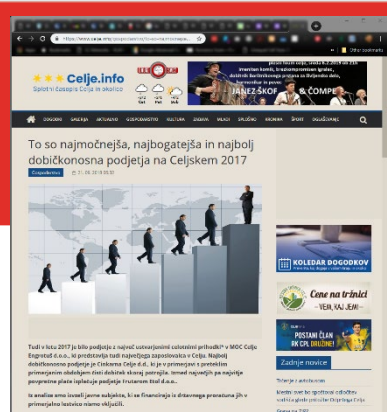
- I google: „*najbolj uspešna celjska podjetja.*“ *[best Celje region companies]*
- I find this: https://www.celje.info/gospodarstvo/to-so-najmocnejse-najbogatejse-in-najbolj-dobickonosne-firme-na-celjskem/

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

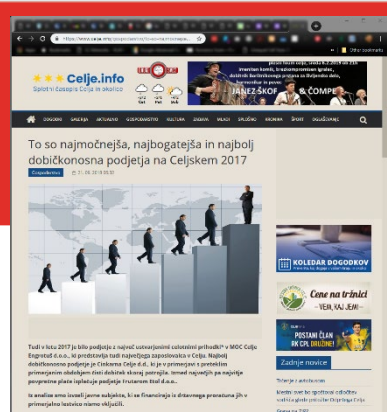
1. Picking the

- I google: „*najbolj* *ies]*
- I find this: https *ocnejse-*
  najbogatejse-in-



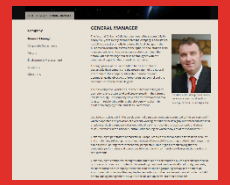


david.hodzic@fri.uni-lj.si



1. Picking the target

- I google: „*najbolj uspešna celjska podjetja.*“ *[best Celje region companies]*
- I find this: https://www.celje.info/gospodarstvo/to-so-najmocnejse-najbogatejse-in-najbolj-dobickonosne-firme-na-celjskem/
- First place is Tuš (its director Mirko Tuš possibly does not live in Celje. I don’t know, but I reject him for that reason).
- Second place is Cinkarna Celje [*Celje zink foundry*]. I’ll OSINT them.

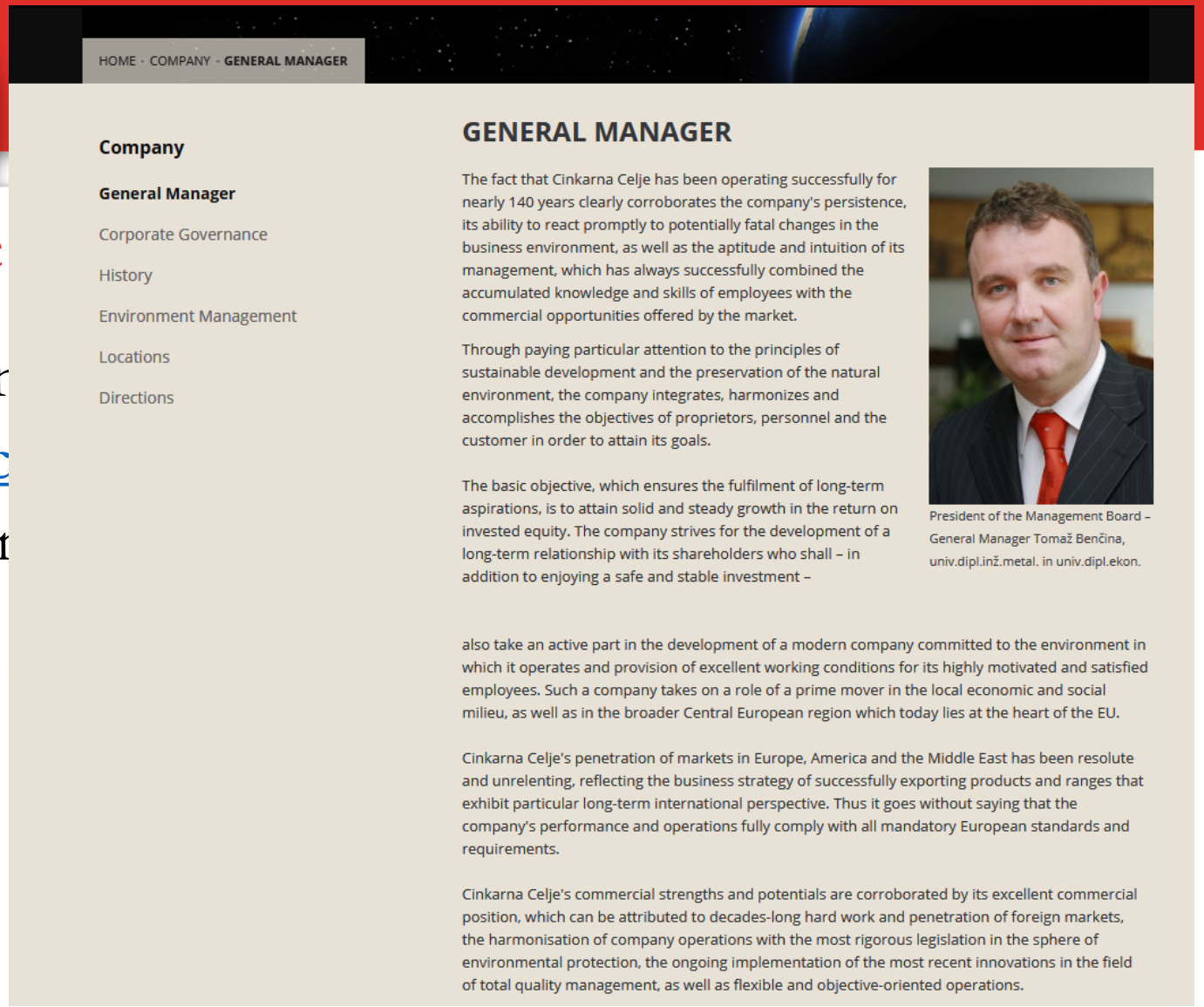


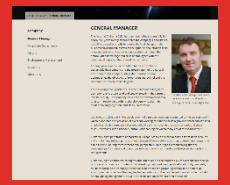
2b. Zbiranje informacij o tarči (OSINT)

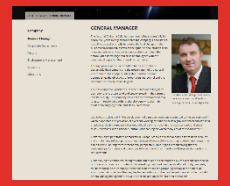
- Who runs Cinkarno Celje?
- http://www.cinkarna.si/en/company/general-manager
-
-
  -
  -
-
  -
  -

2b. Zbiranje

- Who runs Cir
- http://www.c
- Tomaž Benčir
-
  -
  -
-
  -
  -

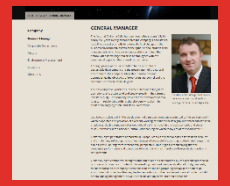






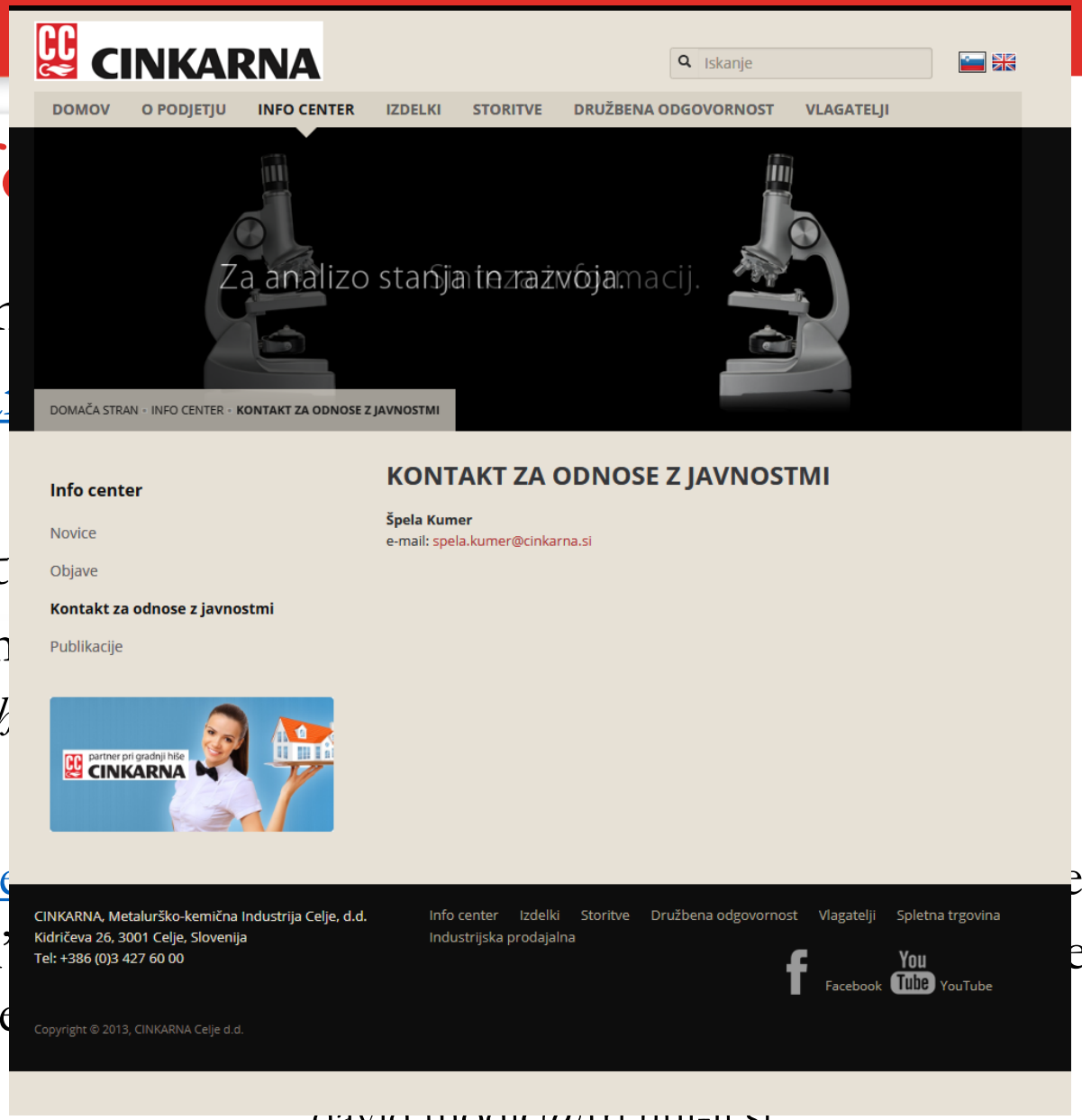
2b. Zbiranje informacij o tarči (OSINT)

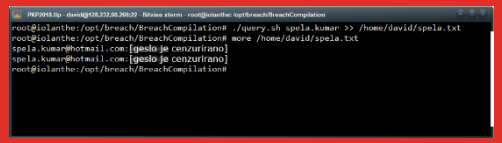
- Who runs Cinkarno Celje?
- http://www.cinkarna.si/en/company/general-manager
- Tomaž Benčina.
- Is he on social networks?
  - Can't find him on Linkedin or facebook.
  - *Reverse image search* of his portrait does not offer any other pages.
- His email?
  - Possibly tomaz.bencina@cinkarna.si (if going by the INFO center page).
  - In the end, I don't care. Because I have his PR person's email. She surely communicates with him or his secretary.



2b. Zbiranje inf

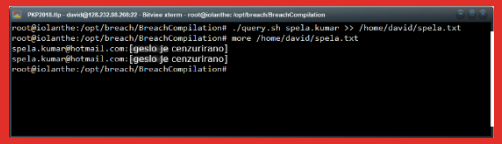
- Who runs Cinkarn
- http://www.cinka
- Tomaž Benčina.
- Is he on social net
  - Can't find him on
  - *Reverse image search*
- His email?
  - Possibly tomaz.be er page).
  - In the end, I don' e surely communicates with him or his se





2c. Breach database

- I have an email: spela.kumer@cinkarna.si
- I look into breach database (*although, I am sceptical*).
- I get a password, but I won't use it. **Why**?
-
-
-
-

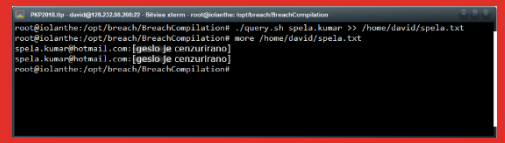


2c. Breach database

- I have an email: spela.kumer@cinkarna.si
- I lo[illegible]

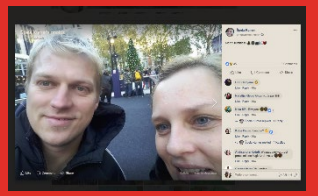
PKP2018.tlp - david@128.232.98.208:22 - Bitvise xterm - root@iolanthe: /opt/breach/BreachCompilation

```
root@iolanthe:/opt/breach/BreachCompilation# ./query.sh spela.kumar >> /home/david/spela.txt
root@iolanthe:/opt/breach/BreachCompilation# more /home/david/spela.txt
spela.kumar@hotmail.com:[geslo je cenzurirano]
spela.kumar@hotmail.com:[geslo je cenzurirano]
root@iolanthe:/opt/breach/BreachCompilation#
```



2c. Breach database

- I have an email: spela.kumer@cinkarna.si
- I look into breach database (*although, I am sceptical*).
- I get a password, but I won't use it. **Why**?
- It's illegal, of course. Active attack.
- I check Tomaž Benčin, but he is not in the breach_db.
- In fact cinkarna.si is not in breach_db.
- But he is on haveibeenpwned.com. So, I know for a fact that tomaz.bencina@cinkarna.si is viable.

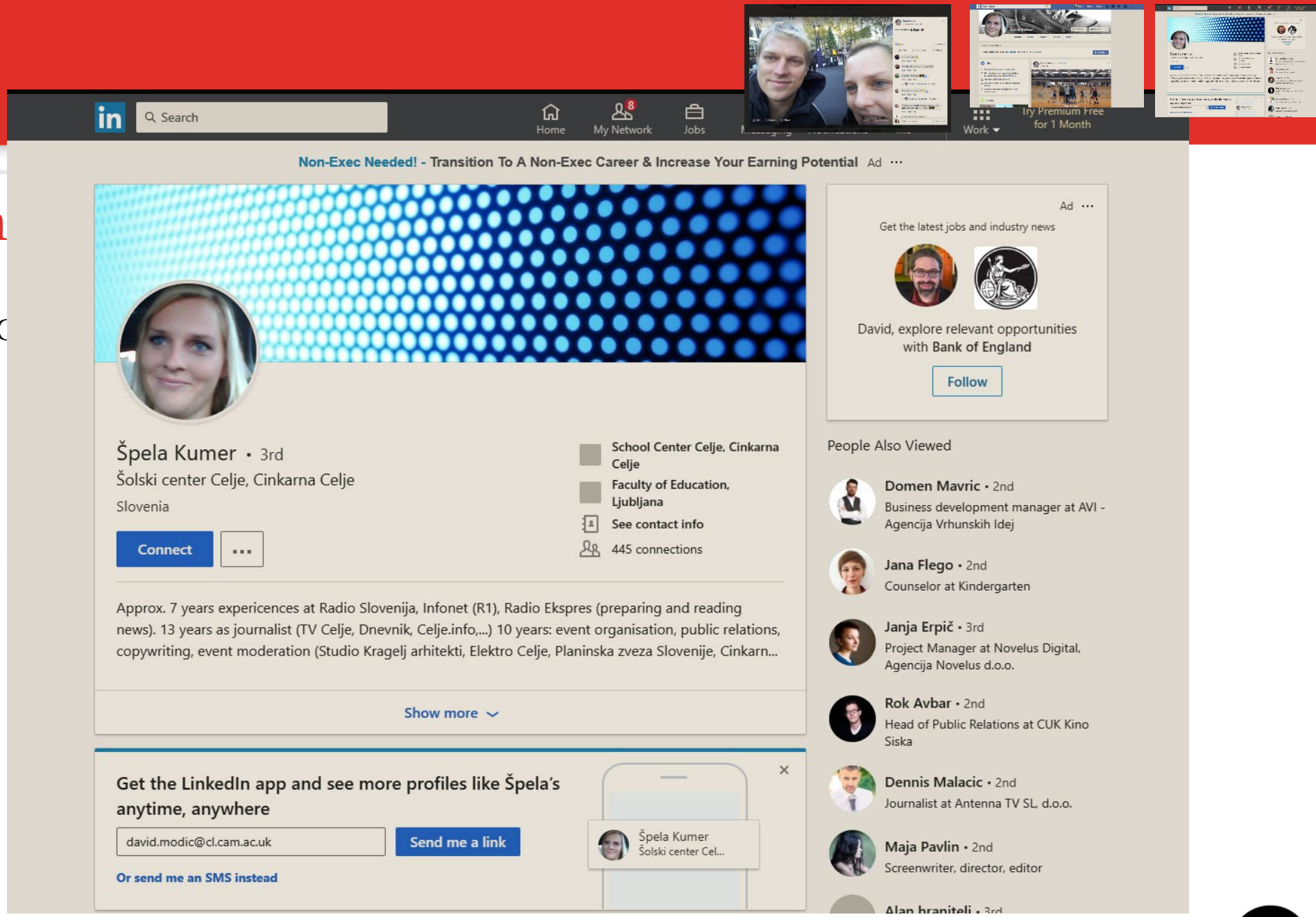


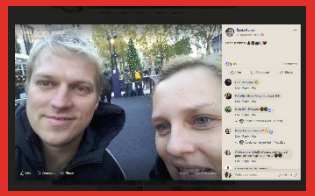
2d. OSINT on the PR person

- Is Špela Kumer on linkedin? Yes.

2d. OSINT on

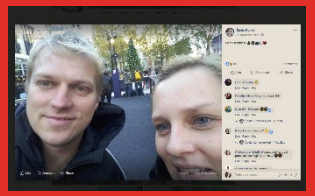
- Is Špela Kumer c





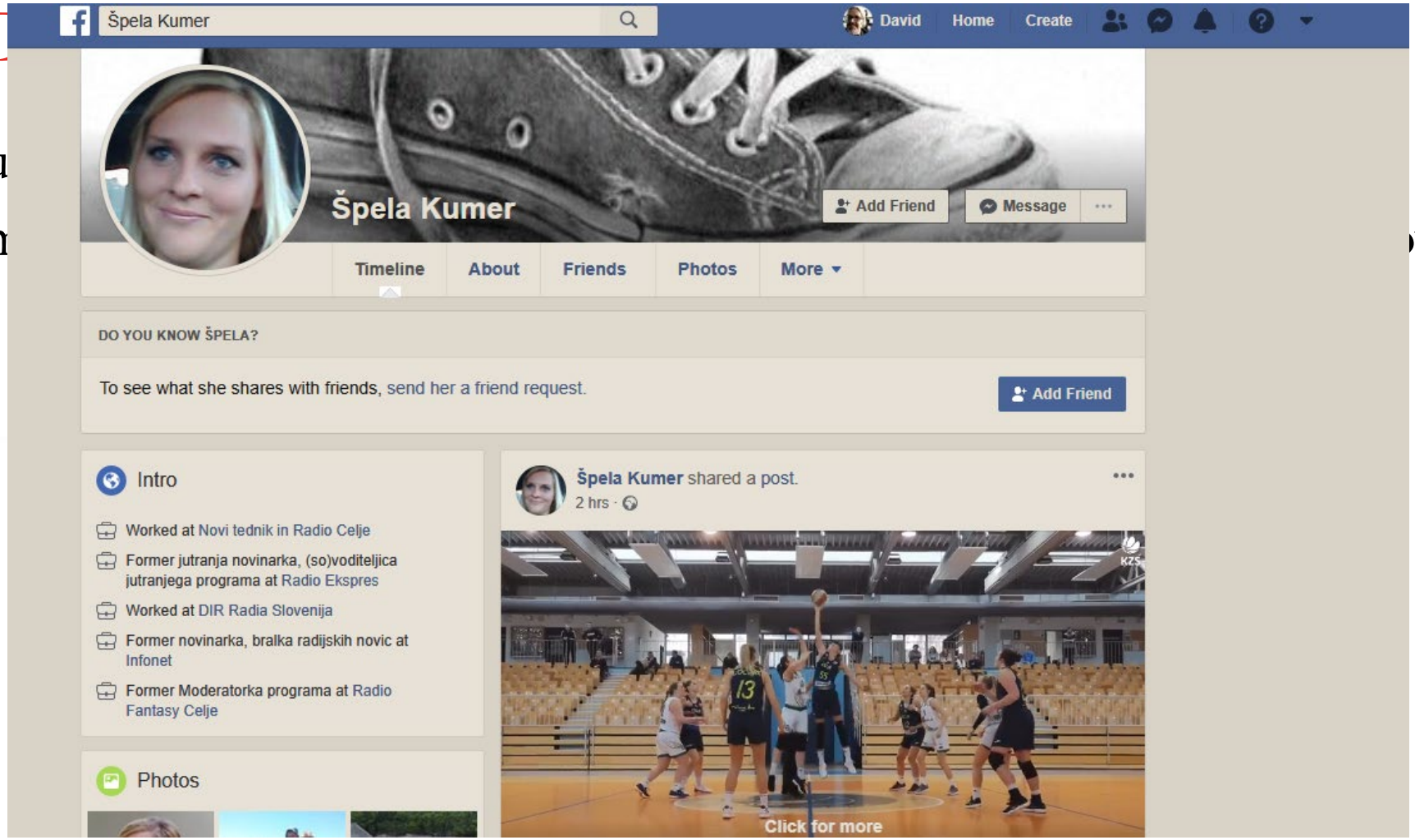
2d. OSINT on the PR person

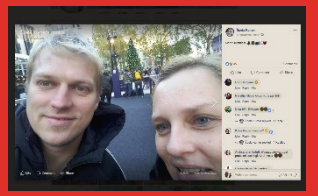
- Is Špela Kumer on linkedin? Yes.
- It is the same Špela – she works in Cinkarna Celje. I have her photo now.
- Facebook?
-
-
-
-
-



2d. OSINT

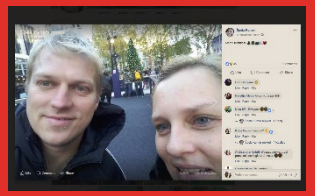
- Is Špela Ku
- It is the san ow.
- Facebook?
-
-
-
-
-
-





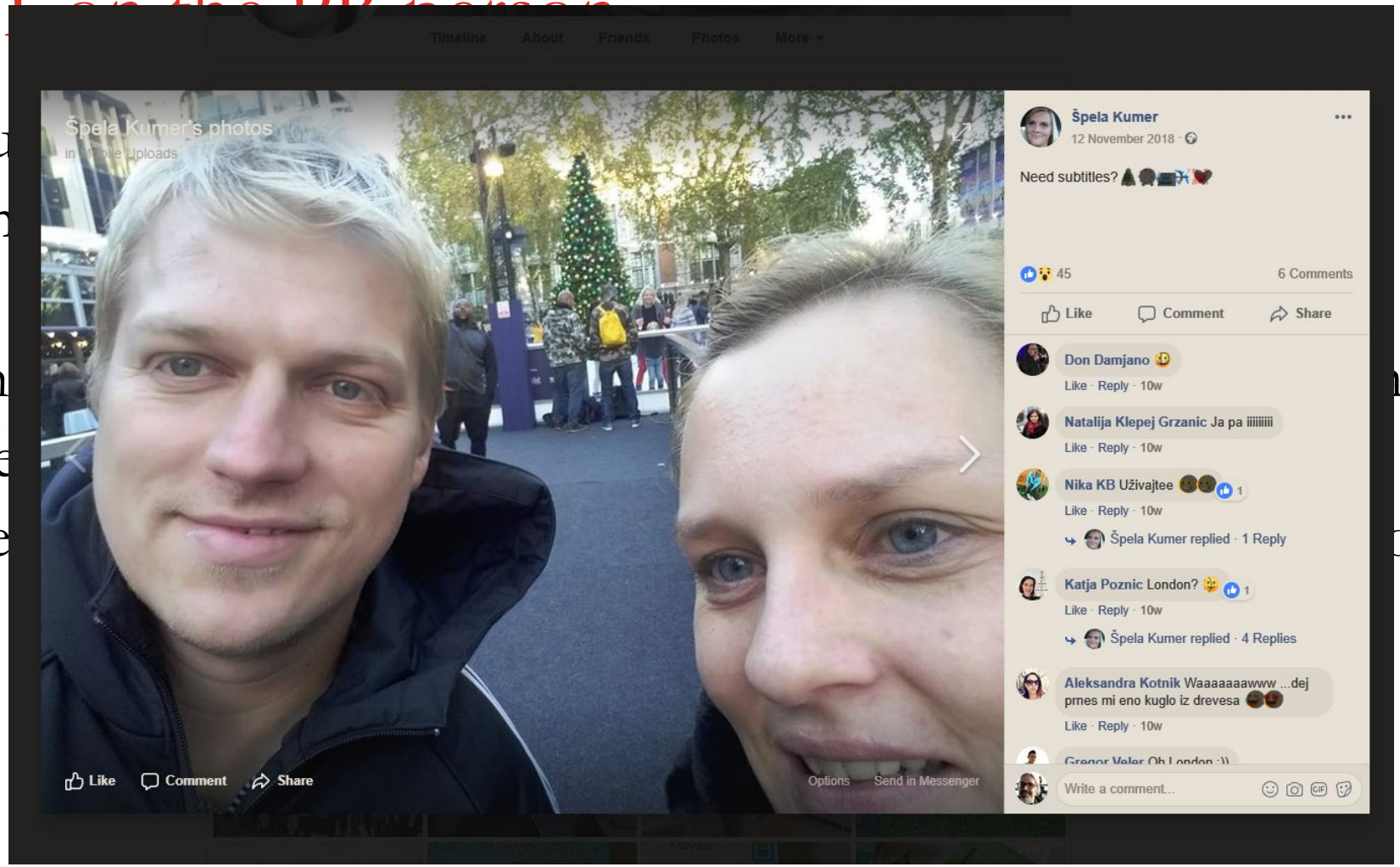
2d. OSINT on the PR person

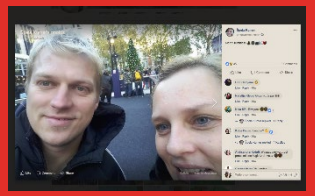
- Is Špela Kumer on linkedin? Yes.
- It is the same Špela – she works in Cinkarna Celje. I have her photo now.
- Facebook?
- Hmm… there is a profile, but it does not state they work in Cinkarna Celje…
- But it is the same person. Same photo on linkedin and on facebook.
- What more? She was in London for Christmas holidays. With someone not tagged.
-
-



2d. OSINT on the PR person

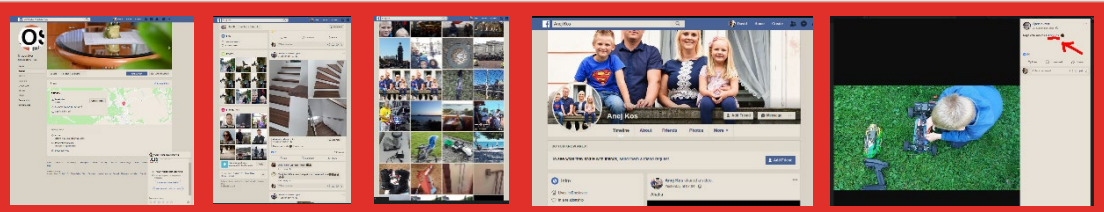
- Is Špela Ku
- It is the san now.
- Facebook?
- Hmm… th na Celje…
- But it is the
- What more one not tagged.
-
-





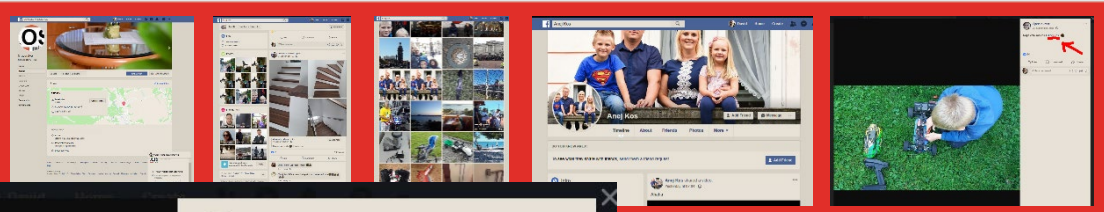
2d. OSINT on the PR person

- Is Špela Kumer on linkedin? Yes.
- It is the same Špela – she works in Cinkarna Celje. I have her photo now.
- Facebook?
- Hmm… there is a profile, but it does not state they work in Cinkarna Celje…
- But it is the same person. Same photo on linkedin and on facebook.
- What more? She was in London for Christmas holidays. With someone not tagged.
- I do a reverse image search, but no luck there.
- But…



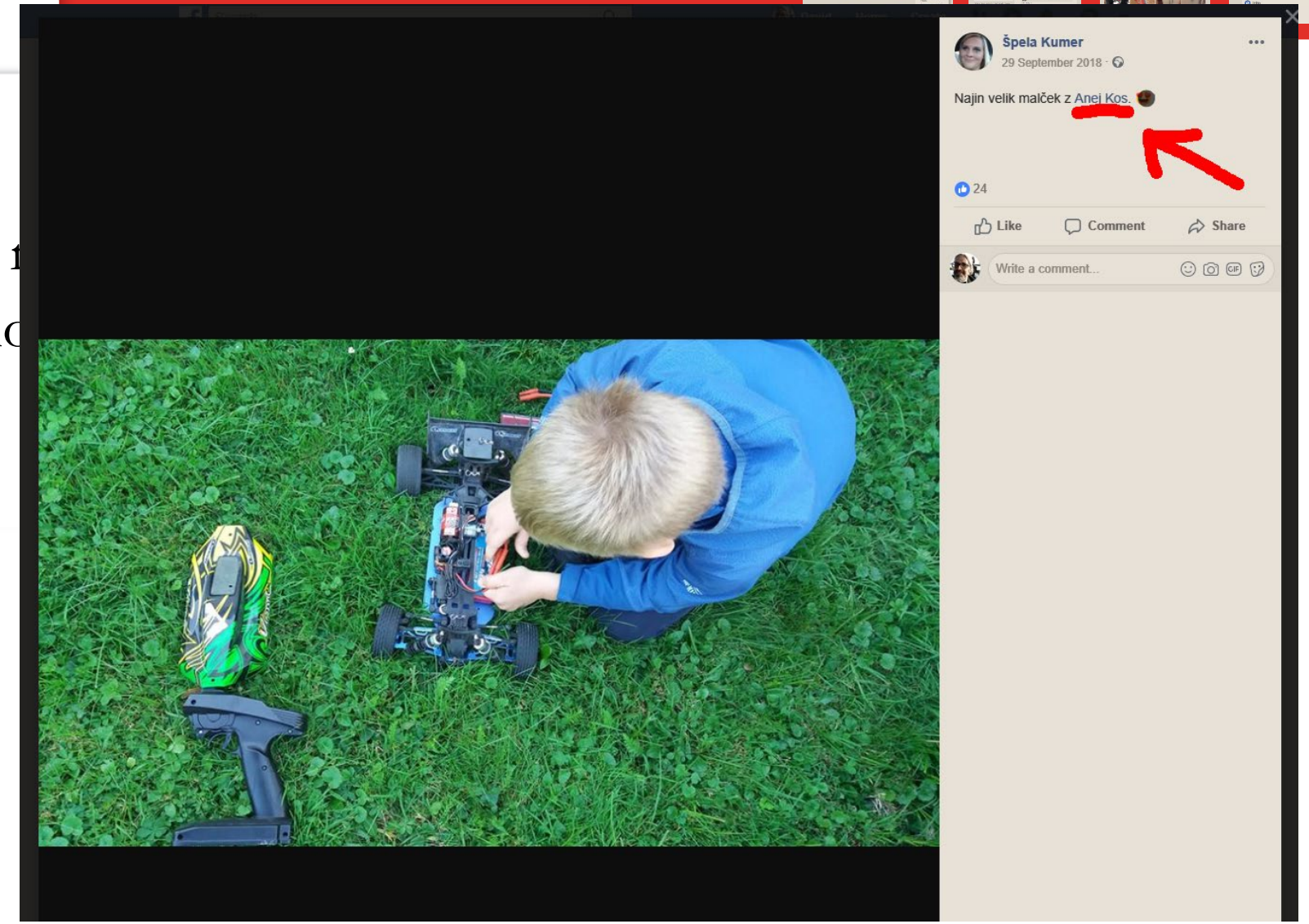
2e. Target (OSINT)

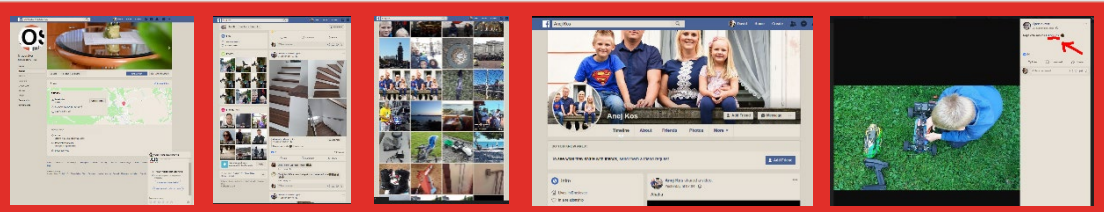
- Špela does not publish faces of her children, wisely.
- On this photo, the dad is linked. Who is this person?



2e. Target

- Špela does
- On this pho
-
-
-
-



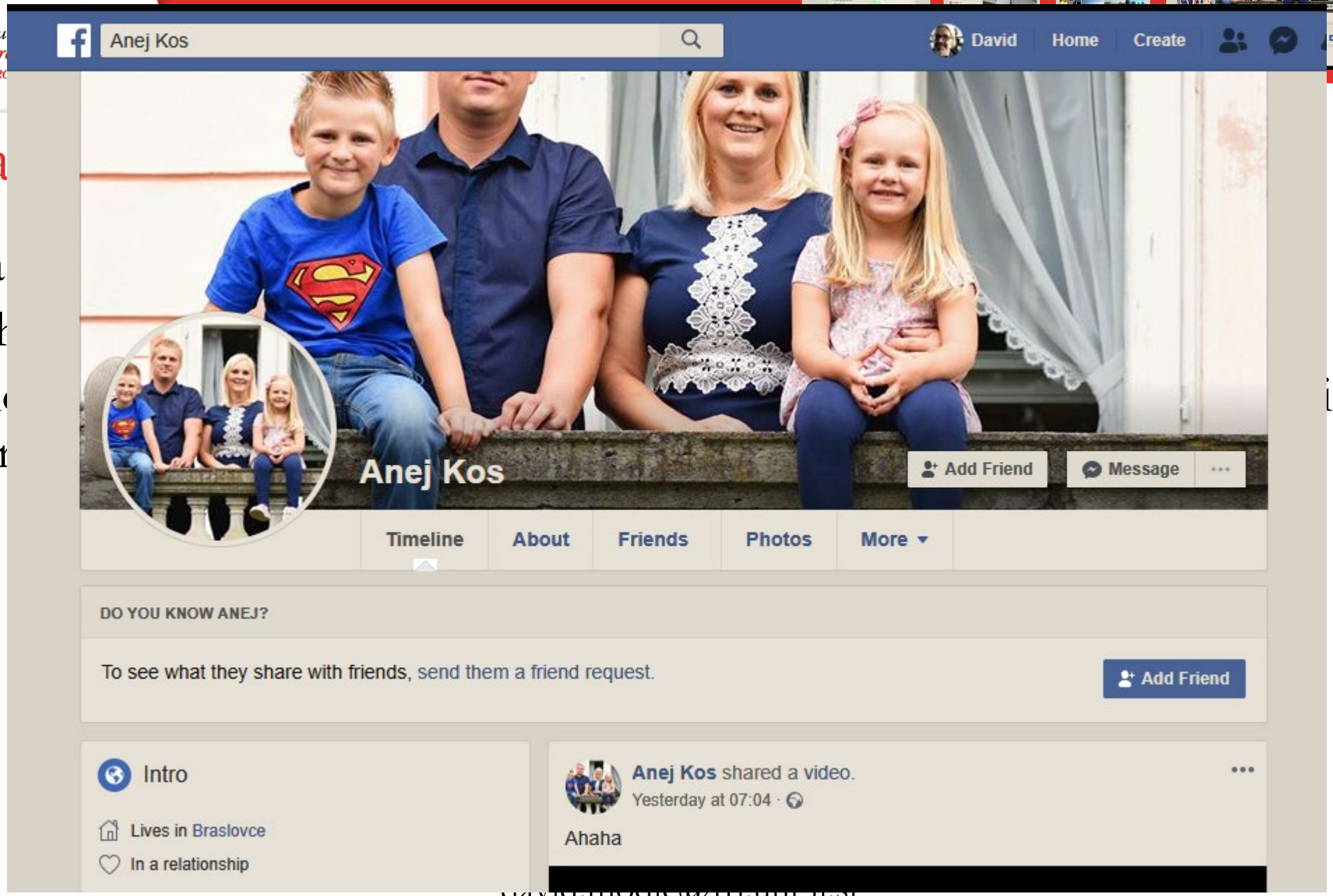


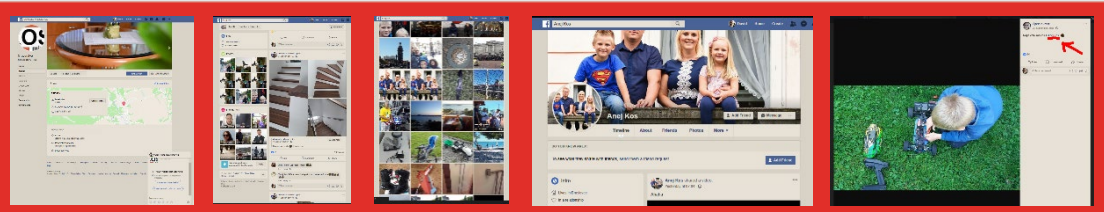
2e. Target (OSINT)

- Špela does not publish faces of her children, wisely.
- On this photo, the dad is linked. Who is this person?
- Obviously, the dad, who is not at all worried that someone might see his children.

2e. Ta

- Špela
- On th
- Obvi is
  childr
-
-
-



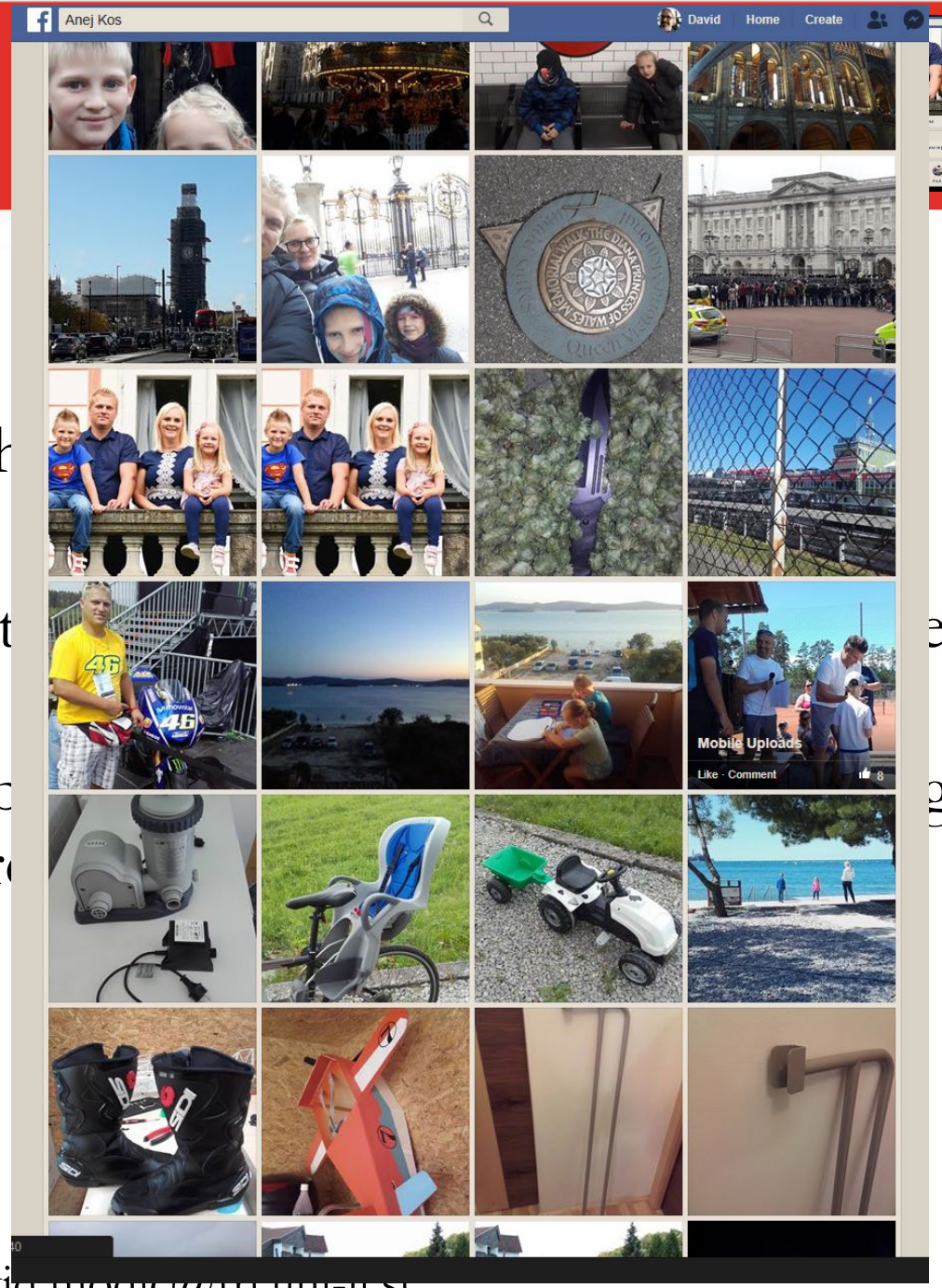


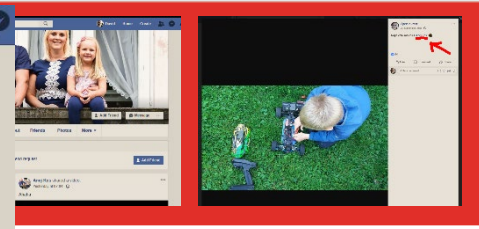
2e. Target (OSINT)

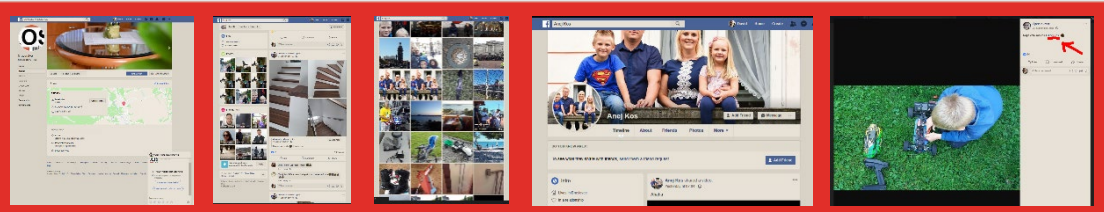
- Špela does not publish faces of her children, wisely.
- On this photo, the dad is linked. Who is this person?
- Obviously, the dad, who is not at all worried that someone might see his children.
- Even better, we find out he is a biker and plays tennis. Reverse image search or Geo Tagging might tell me where they go on holidays.
-
-

2e. Target (OSINT)

- Špela does not publish faces of h
- On this photo, the dad is linked.
- Obviously, the dad, who is not at ee his children.
- Even better, we find out he is a b ge search or Geo Tagging might tell me where







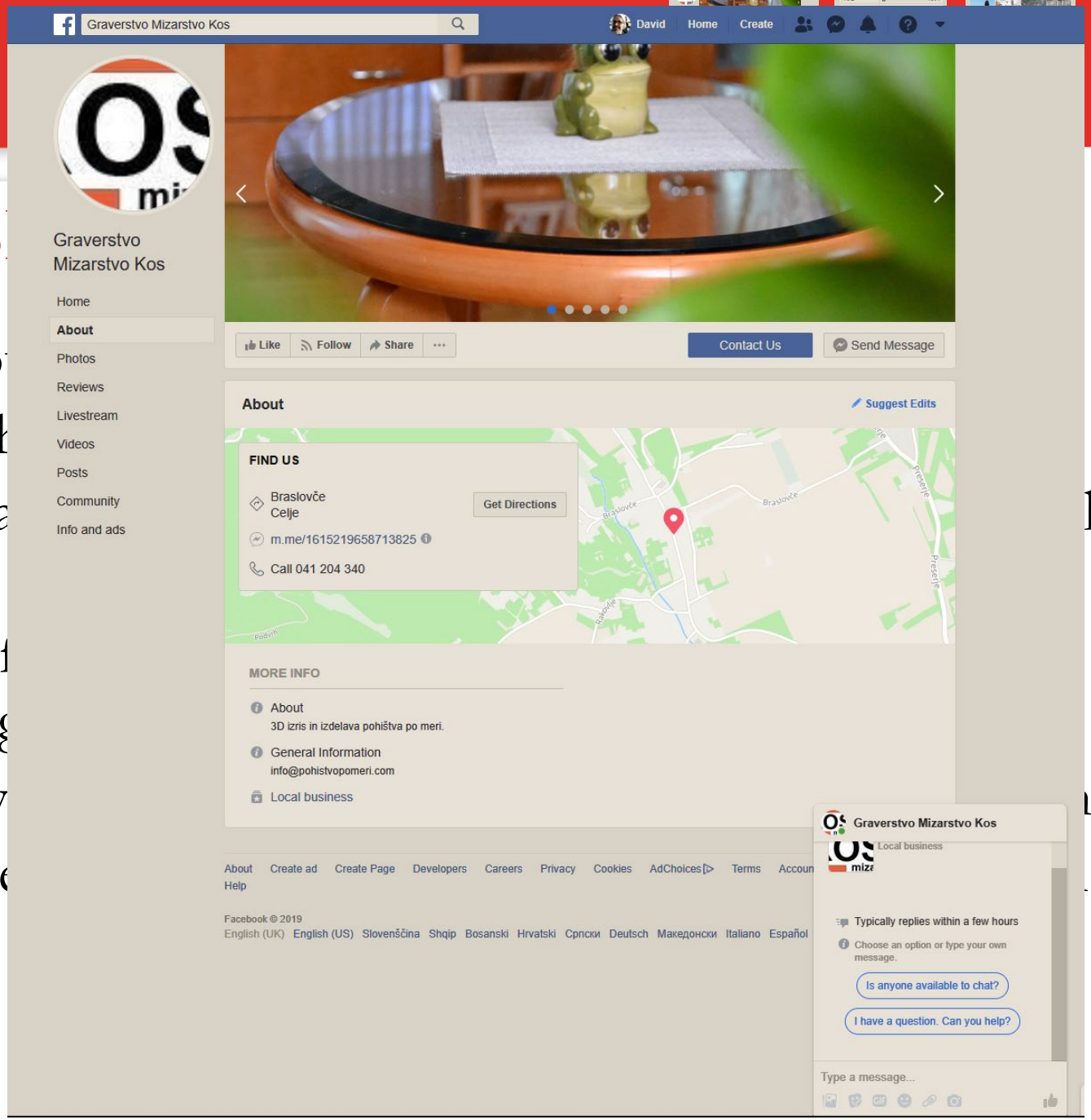
2e. Target (OSINT)

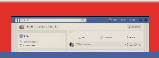
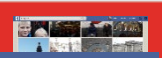
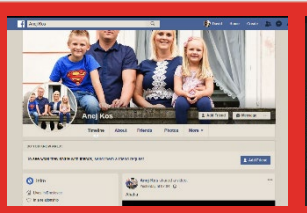
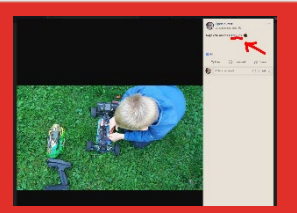
- Špela does not publish faces of her children, wisely.
- On this photo, the dad is linked. Who is this person?
- Obviously, the dad, who is not at all worried that someone might see his children.
- Even better, we find out he is a biker and plays tennis. Reverse image search or Geo Tagging might tell me where they go on holidays.
- I see where he works. Has a woodworking shop. Works from home.
-

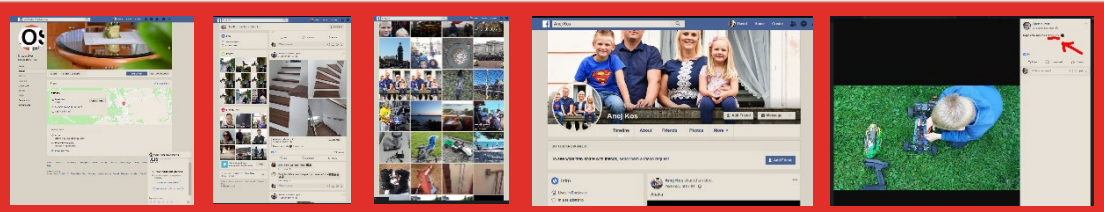
Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

2e. Target (OS

- Špela does not p
- On this photo, th
- Obviously the da ht see his children.
- Even better, we f image search or Geo Tagging mig
- I see where he w ome.
- Therefore, I have ey are away.





2e. Target (OSINT)

- Špela does not publish faces of her children, wisely.
- On this photo, the dad is linked. Who is this person?
- Obviously, the dad, who is not at all worried that someone might see his children.
- Even better, we find out he is a biker and plays tennis. Reverse image search or Geo Tagging might tell me where they go on holidays.
- I see where he works. Has a woodworking shop. Works from home.
- Therefore, I have the family home address. And times when they are away.

So, what do I have now?

- Email from the PR person for CC.
- I have their facebook page, home address, photos of the family, name of the partner, his hobbies. Enough for now.
- I would be able to almost certainly find also:
  - Birthdates of the children, names of children, names of extended family, their addresses etc.
- From now on, there would be active measures involved.
- I am presenting attack vectors, *but I did not do them!*

3a. Active measures I.

- I would google „*Osnovne Šole v Celju in okolici*“ *[Primary schools in and around Celje]*.
- First search would be for *O.Š. Braslovče*, a school in their home village. Because the kids are probably there.
- I would visit the school webpage and look for staff info & publications & photos of events. If they do have photos, fine. Not a deal-breaker either way.
- If I find class photos, then I know who the teacher is and which grade the children are in. I might find out their names too.
- Let’s say I found a class photo. Therefore, I know it is the right school.
- Let’s pretend that the kids are in the first and third grade.

3b. Active measures I.

- I call the school (the phone number is on the web page). I ask for the school advisor / psychologist (their name is also on the web page).
- I say: „Hello. I am calling from the police station Celje, my name is Lovro Božič *[I could find the real name too]*. There is an incident in Cinkarna Celje that is still in progress. I am afraid I cannot disclose more. Some of the employees cannot be contacted. The mother of two of your pupils in first and third grade, Špela Kumer, who lives at *[XX]* is one of those people. We called her partner, *[IME]*, but he is also unavailable. Can you please check whether the kids are in class, as a matter of some urgency. I need to confirm their names too, please.“
- And I would have their names. It is possible that they would tell me their names of their own volition, e.g. „Oh yes, you mean Johan and Benedeta? They are here, yes, I saw them earlier.“

4a. Attack vector II.

- An email to Špela:

„Hi, I am *[name of the advisor]*,

I apologize for writing to you directly, but there was an unfortunate event at school today. Your daughter, *[name]* from class *[X]*, was involved as a bystander.

Do not worry, [name] is completely fine. She was not actively involved. She might not even realize that she witnessed the event. I would ask you not to mention it, unless she does. I still thought you wanted to be informed about these events. I do not want to disclose more, but a fuller report is available here: [URL].

Kind regards, [etc, etc]”

4b. Attack vector II.

- The link would install a trojan package, like *kovter* (link to the description on moodle). It would collect access codes.
- *(optional): As Špela, I write to the sysadmin and complain that my machine is acting up. What did they change again?* Sooner or later I find out what is allowed through their IDS / firewall and what is not. And whether they have a spam/AV filter.
- I access Špela's work account. I check who the recipient/approver of press releases usually is: The secretary to the CEO, or the CEO? I analyze the writing style – first name basis, how formal, any recurring phrases?

5a. Attack vector III.

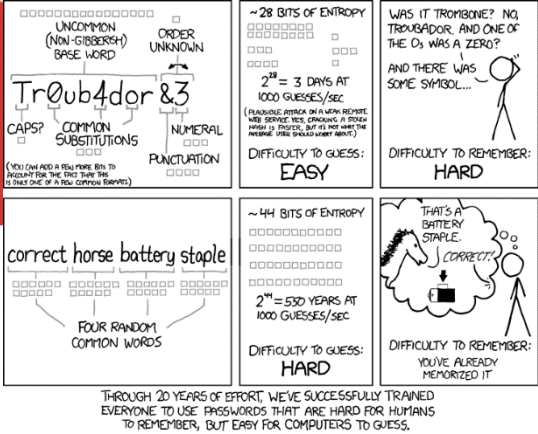
- Let's say Špela talks to the CEO directly. If not, I would do the same thing to whomever she does communicate with.
- Špela sends an email to the CEO. The writing style and formality is copied from previous email exchanges.

„Dear Tomaž,

Sorry for bothering you again, but the journalists from Večer are bothering me constantly (see our previous exchanges about that, the latest dated *[X]*). I wrote the following press release and I wanted your approval (pdf attached). Please read it and let me know whether I can release it.“

5b. Attack vector III.

- Once Tomaž opens the pdf it inserts malware on his machine too.
- I then own Cinkarna Celje.
  - I can request a large sum of money to be transferred to an off-shore account (once I made sure Tomaž is not available).
  - I can slowly syphon trade secrets and IP from CC and sell it to other foundries.
  - I can, if hired to do so, sabotage parts of the production.
  - I can use CC infrastructure to attack other companies (for DDOS, let's say).
  - I can destroy the reputation of CC.
  - I can redirect the salaries of the employees to accounts in Russia, China, South Korea, etc.



A few points

- I found a password in the breach database. It was simplistic. That tells me how security savvy my direct target is (not very).
- I know that operational security of the PR person is weak.
- From (optional) discussions with the sys-admin, I would find out much about the security make-up of the company.
- We have discussed this already: Panda security claims that 85% of users use the same password for their e-commerce log-ins (link on ucilnica).

A few more points

- Operational security is hard (as discussed in previous lectures and this one too):
- I made assumptions based on that:
  - In spite of Špela not listing her employer on facebooku (shrewd),
  - … she kept the same photo across profiles *(operational fail)*.
  - Even though she knew not to post identifiable photos of her kids on facebook (shrewd), *she still tagged* someone who did not care about operational security at all (*operational fail*).
  - I know when she is away and where, from Facebook (the photo from her trip was posted *while* she was away).
  - While she does not list her address, her partner did.
  - And so on…
- I could also try to reset her passwords, send her an email from HMRC Customs and Excise (she was in the UK recently),

A short break

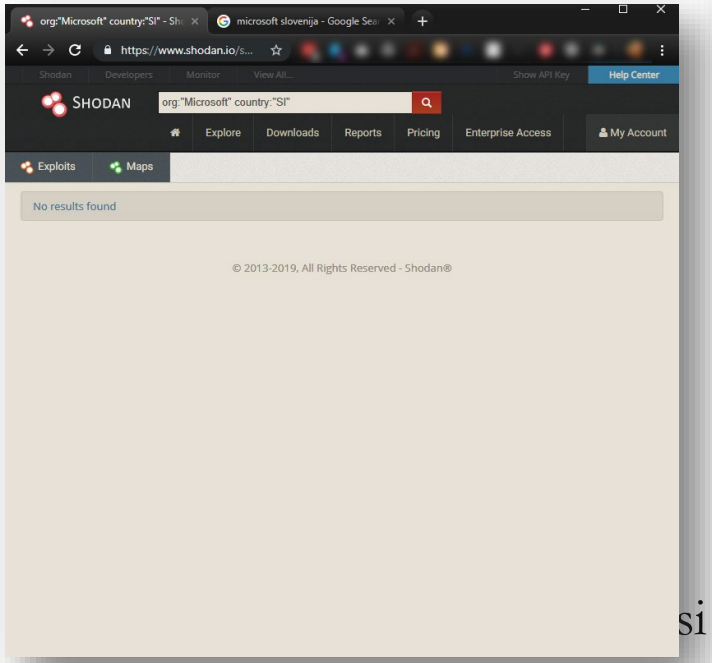
- Let's take 10 minutes and then move on to another practical example. Agreed?

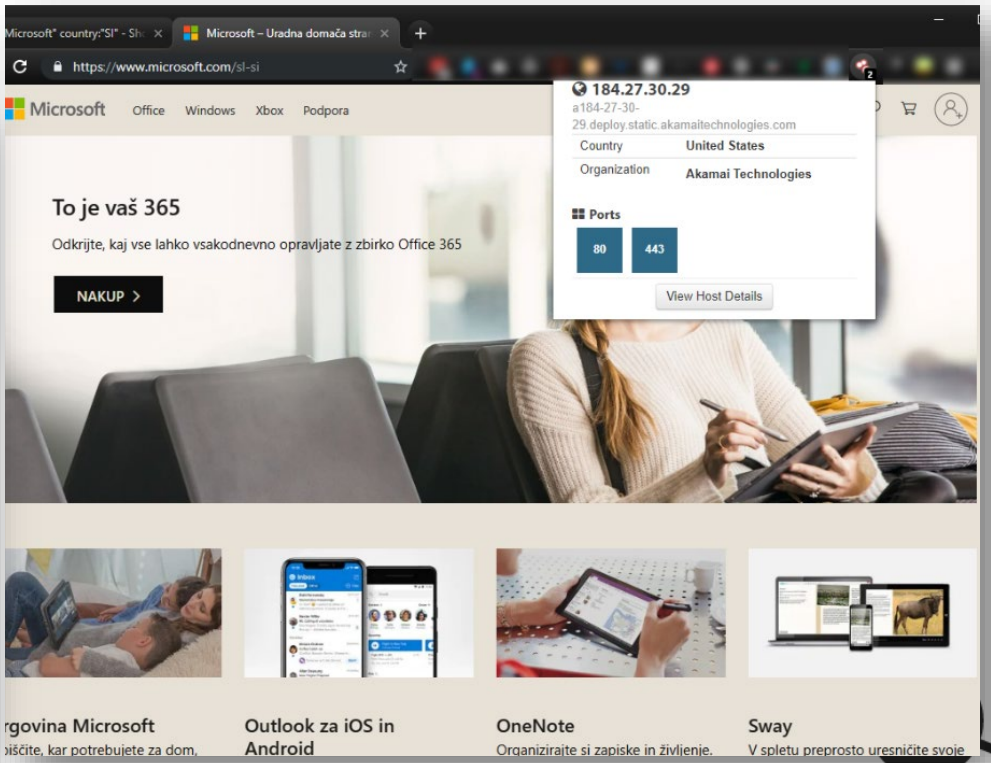
Threat model

- 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 a passive scan or two as a hail mary.
- (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.

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.

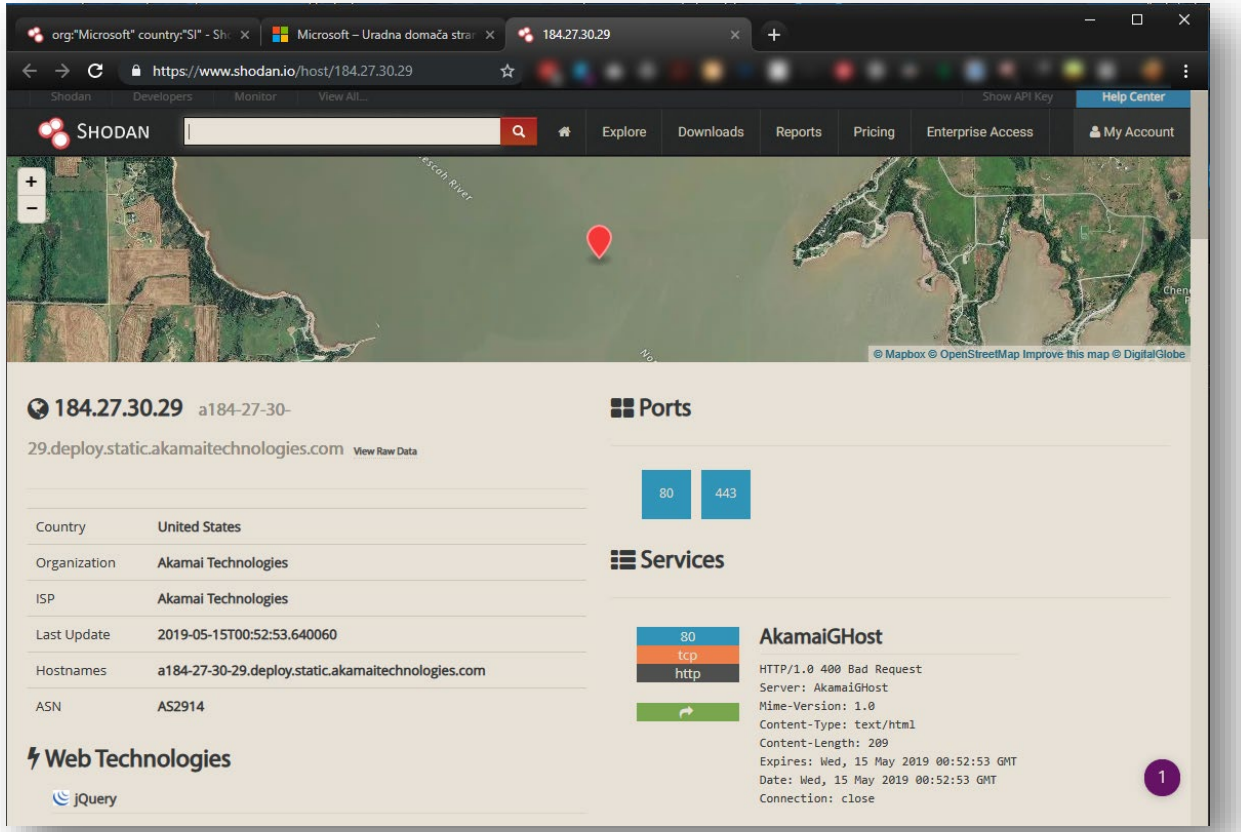


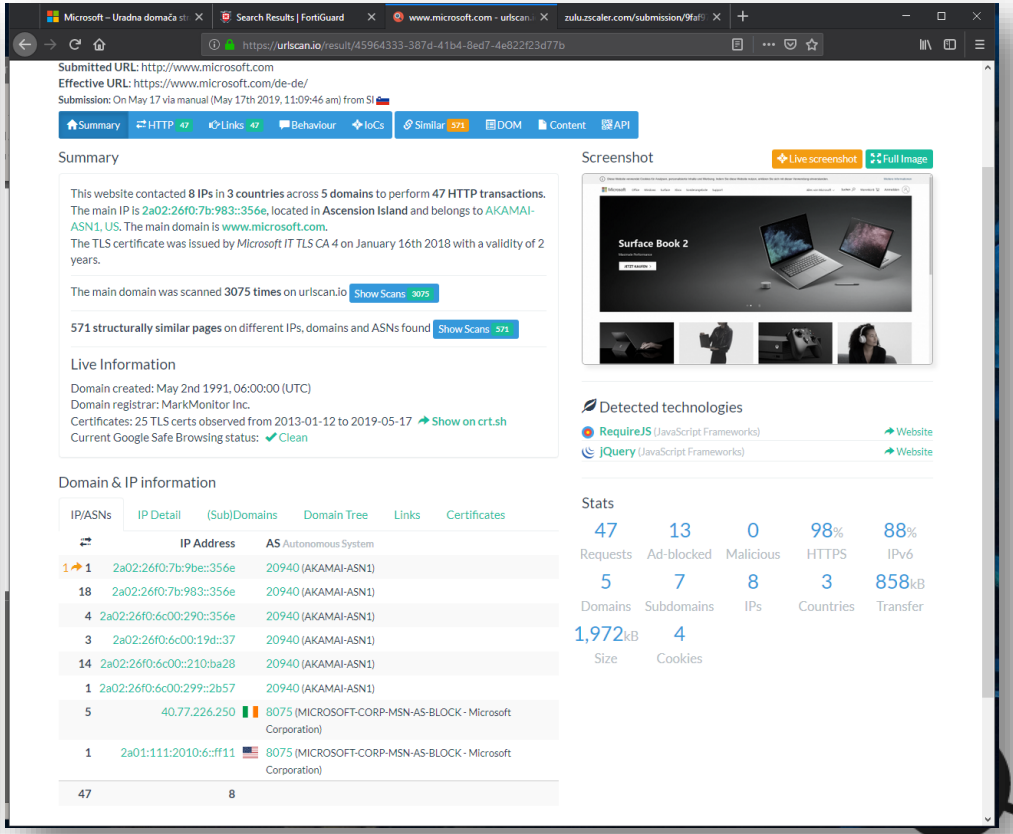


Step 1. Continued - OSINT.

3. Shodan host info shows that the server is nicely obfuscated – located somewhere in the ocean...

4. I get some fairly useless info from urlscan. I do now know IPv6 is enabled and used by default on the MS servers.

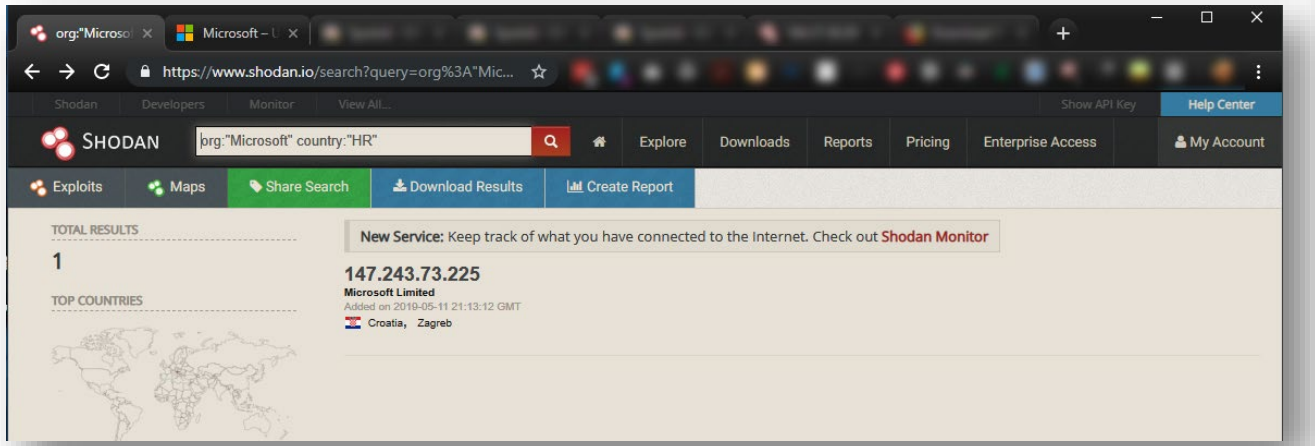


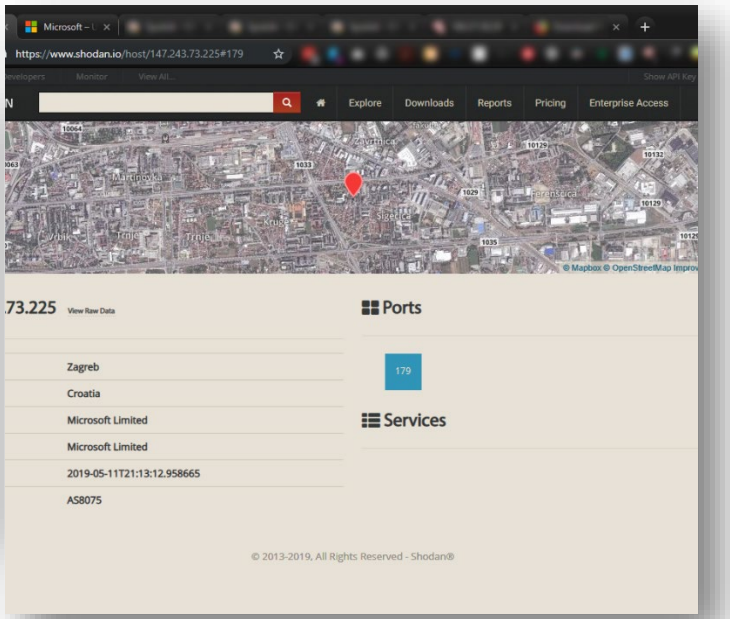


Microsoft Croatia

THIS HAS NOTHING TO DO WITH OUR INVESTIGATION. STILL MIGHT BE OF INTEREST

- Shodan search for Microsoft presence in Slovenia yields no results. **However, there is one server in Croatia! I doubt this is actually owned by Microsoft.** Mostly because I do not think MS is a Limited company (**LTD**), I think it is **PLC.**
- It has one port opened – 179, which is a gateway forwarding port. So there is one server in Zagreb (in a residential area) that serves as an entry portal into Microsoft network? That seems fishy.





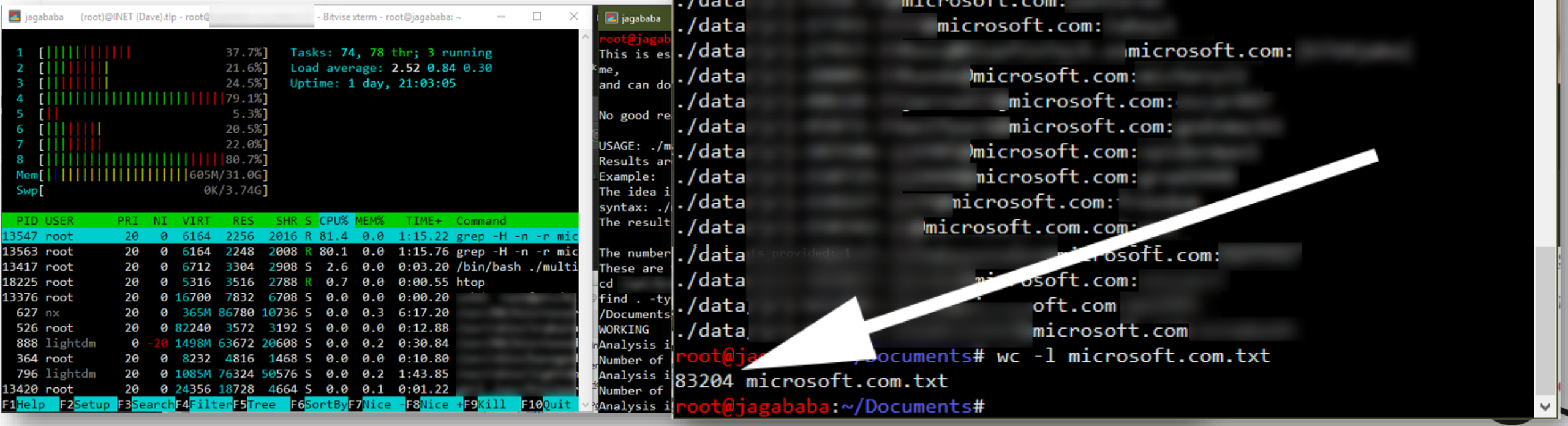
Step 1. Summary

- *Looking at topology and infrastructure overview yields no usable attack vectors.*
- *I would be **very** surprised if it did. Microsoft is probably constantly scanned and prodded so going through their main web server is probably insane.*
- *That is why I did this part fairly half-assed. Did not expect to find anything.*

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

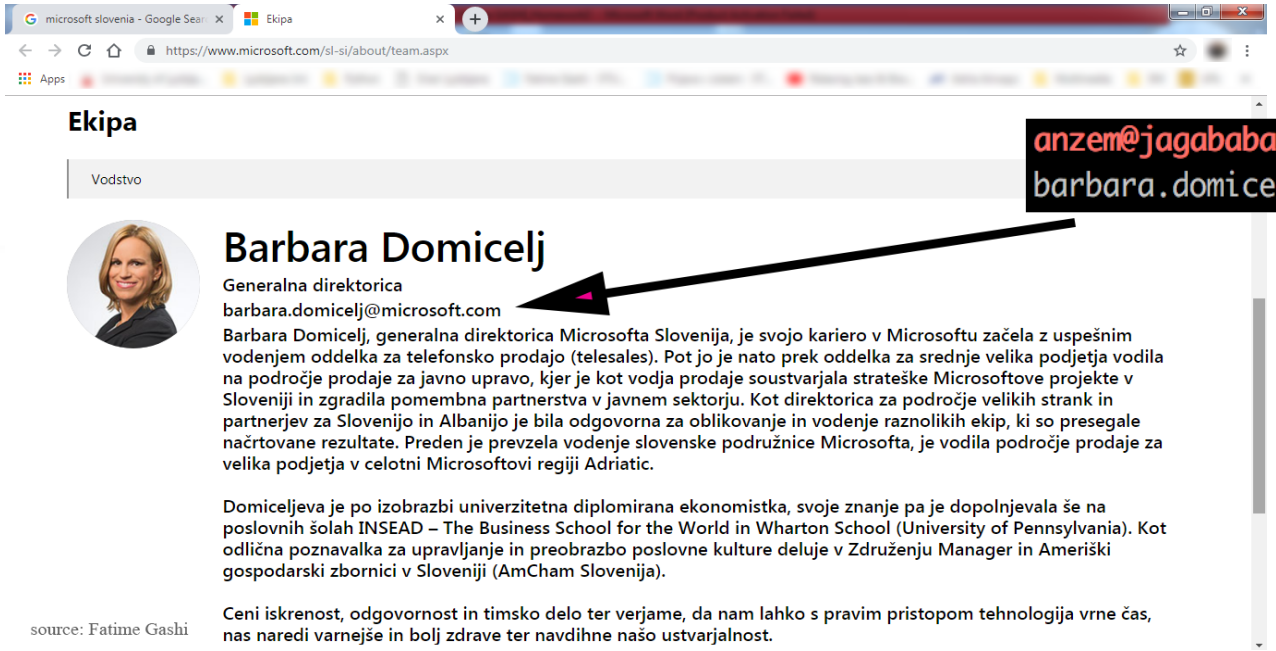
Step 2. OSINT 1.

- What does the breach database say about microsoft.com emails?
- There are a bit more than 83000 entries with the domain Microsoft.com in the email address.



STEP 2. OSINT 2

- The CEO of MS.SI is Barbara Domicelj. Her email address is apparently barbara.domicelj@microsoft.si
- The breach database offers one hit for barbara.domicelj@Microsoft.si.



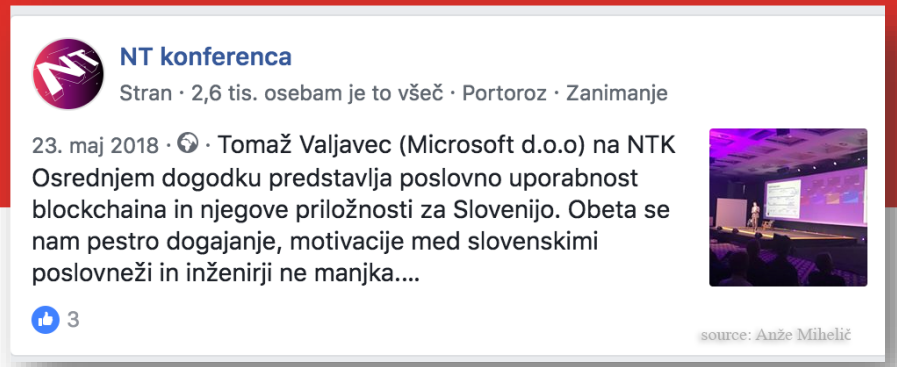

```
anzem@jagababa:/opt/breach/BreachCompilation$ sudo ./query.sh barbara.domicelj
barbara.domicelj@microsoft.com:A[redacted]1
```

source: Anže Mihelič

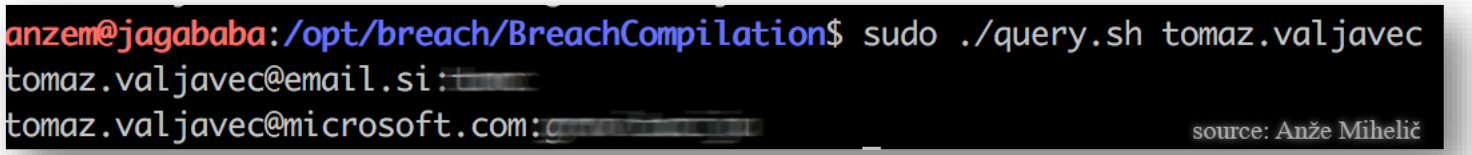
STEP 2. OSINT 2

- Now. I have no idea if this password still works or not.
- **Neither me, nor my students tried it**.
- This is quite probably not her work account password. *If it is, I despair. Eight characters, first uppercase, last number… Brute-force time is about 20s I think.*
- ***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 Barbara constructs passwords and (b) there is a chance that I can log-in with this password into something valuable.***

STEP 2. OSINT 3.



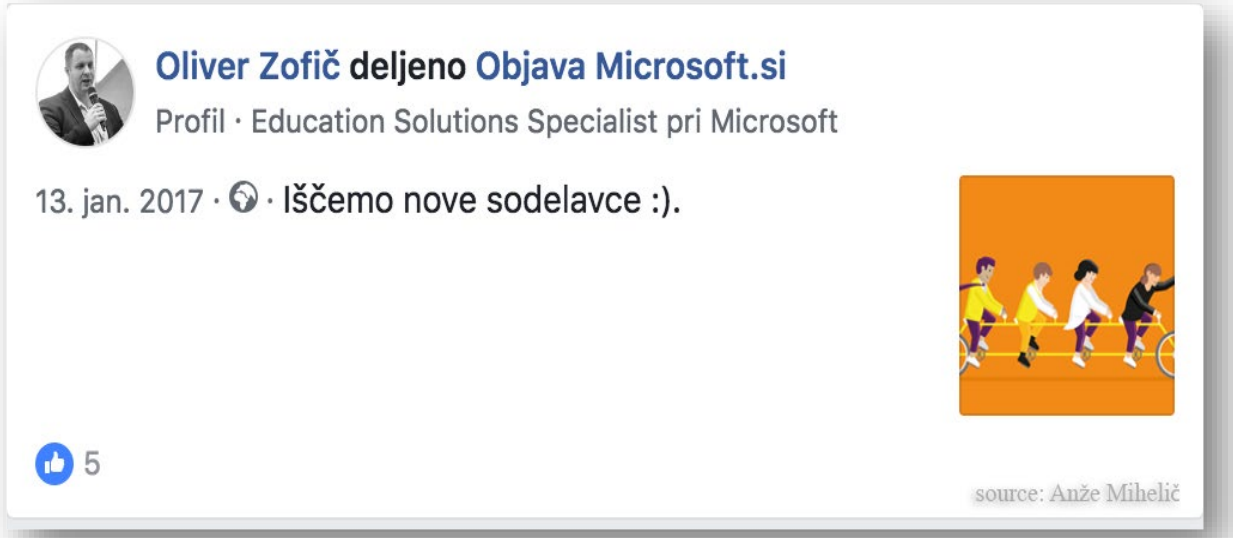
- Microsoft is not terribly forthcoming about their employee structure. However, it seems that Microsoft Slovenia is organising a conference and the regional leader for solutions in the cloud is giving a keynote…..
- The breach database offers two hits for tomaz.valjavec (password is redacted only on the slide).
- Same caveats apply as with Barbara Domicelj.
- However, one password is five characters long and the other is a dictionary word. This is an OPSEC fail.



STEP 2. OSINT 4.

```
anzem@jagababa:/opt/breach/BreachCompilation$ sudo ./query.sh oliver.zofic
oliver.zofic@gmail.com:[redacted]
```
source: Anže Mihelič

- **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.

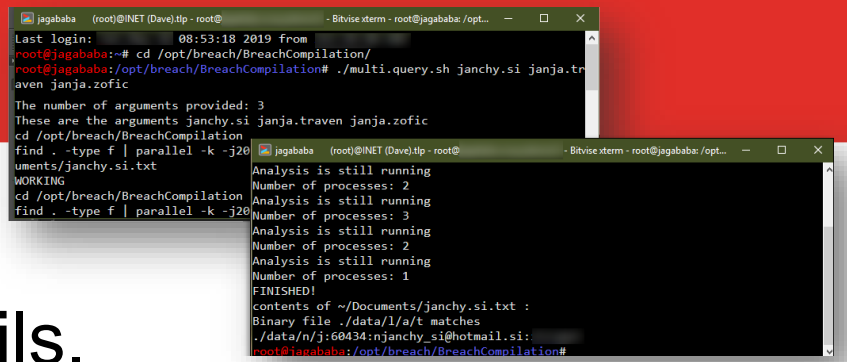


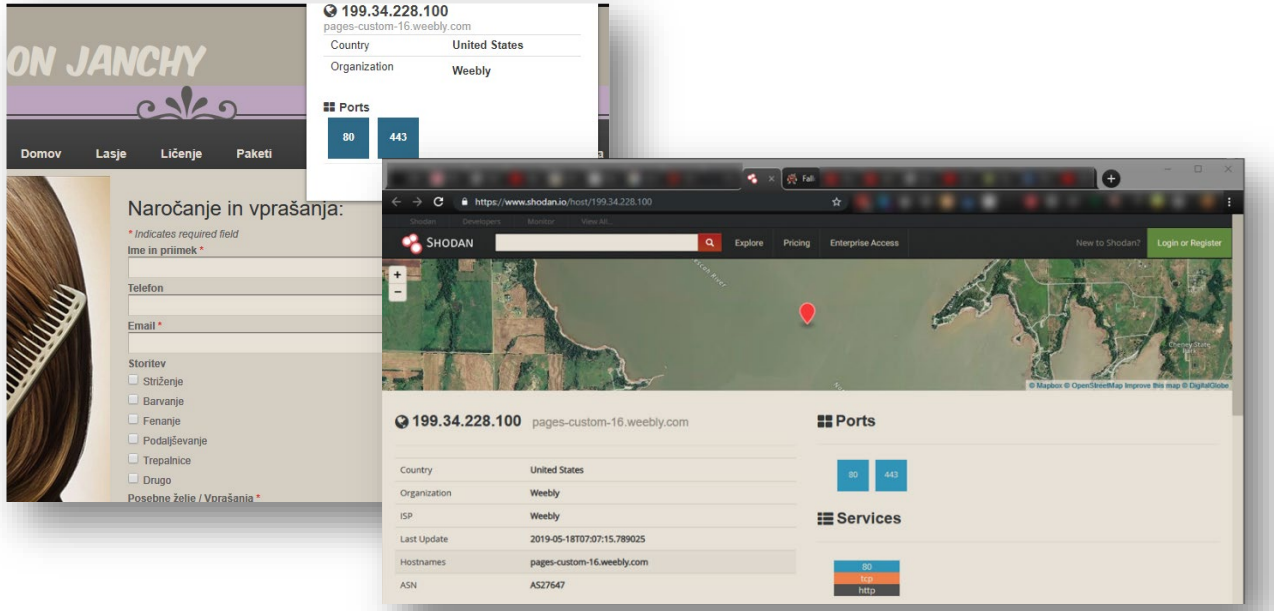
STEP 2. OSINT 4.

- 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.

STEP 2. OSINT 4.

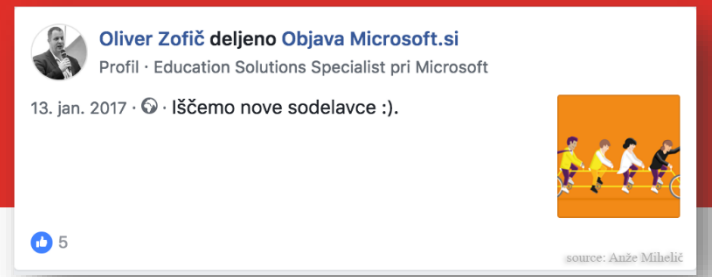
- Salon Janchy yields Janja's work/contact details.
- Shodan gives potentially exploitable info (see attack vectors)





ATTACK VECTOR 1. mechanical attack

- This is completely pointless at this stage.
- Microsoft Slovenia does not seem to have it's own infrastructure that is publicly accessible. The servers seem to be in the US.
- I am more than certain that Microsoft protects itself religiously. They are a frequent target and the reputational fallout from a successful breach would be catastrophic.
- One could try to log-in into various services with usernames and passwords from the breach database.
- Remember, we have details for one Barbara Domicelj's account.
- Also, operational security is *hard*.

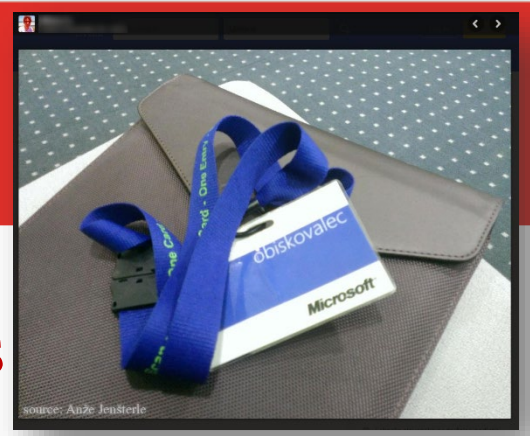


ATTACK VECTOR 2a. Gain physical access

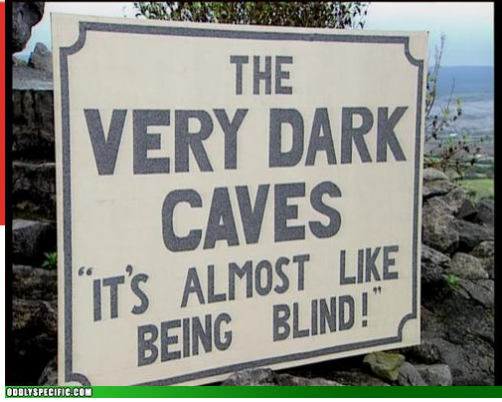
- Every once in a while, Microsoft Slovenia is hiring.

1. Gather OSINT on the hiring committee. Find their hobbies and their attitudes.
2. Create a CV which shows that you share the same hobbies, think all non-technical people are morons (or not, depending on OSINT), show that you were educated at the same places as the hiring team, mention examples of good practice from the companies the hiring committee worked for before. LIE. A lot. The objective is not to get hired, only interviewed.
3. Get invited for an interview. GAIN ACCESS to the building. Do one of the following (depending on opportunities):
   - Get a visitors card, skim it, create your own for later use.
   - Scan networks from the inside, while you wait, check for wireless vulnerabilities.
   - Leave lots of rubber duckies around.
   - In the interview, provide a usb stick with "samples of code" or "supporting documentation" to the team.
   - Make note of physical vulnerabilities (monitors towards outside windows, opportunities to eavesdrop through parabolic antennas, tailgating policies).

ATTACK VECTORS 2b-e. Gain physical access



- What a visitors badge probably looks like: https://foursquare.com/v/microsoft-slovenija/4b5de9c8f964a5204f7329e3?openPhotoId=52b431ab498e65000783d533
- Spoof an email from someone requesting access for you.
- Do physical surveillance, find out when deliveries are and by which company (DHL, FEDEX, GLS …). Show up in a uniform, deliver a package containing malware to someone who works there. Repeat until getting a ping-back.
- Spoof an email from someone to their secretary, phish the secretary.



ATTACK VECTOR 3. Exploit family - groundwork

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

ATTACK VECTOR 2f. Gain proxy physical access

1. Gain physical access to salon Janchy. Find an opportunity to insert a rubber ducky / malware package / keylogger into the system.
    1. One way to go about it would be to simply get a hair cutting appointment.
    2. 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.
2. Another solution would be to send phishing links in the comments section of the "making an appointment" web form.
3. The overall goal would be to gain access to Janja's Mailbox.

ATT. VECT. 3. Exploit family – exploit 1 (petty cash)

1. Janja (we have her mail and business address) receives an email from the *"information commissioners office"*.
2. In it, Andrej Tomšič (*actual ICO deputy*), tells her the ICO is about to start an investigation into the GDPR breach and outlines the reasons.
3. Janja is told that she should *immediately provide a privacy notice* on her page and pay a fine, before she gets into real trouble.
4. The fine is let's say, 500 EUR. It is not worth contesting this as any lawyer would charge more.
   a. The email contains a link to a "*form*" one needs to fill out. *Drive by malware*. PWNED.
   b. 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.
   c. 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.

ATT. VECT. 3. Exploit family – exploit 1 (petty cash)

- **This is truly viable, yes.** However:
- Impersonating an official (2.) carries a jail sentence of up to **1 year** per offence (KZ-1, §305).
- 4a and 4b are both unauthorized intrusions into a computer system, which carries a jail sentence of **1-5 years** (KZ-1, §221 or §237). Also, possession of hacking tools which carries a jail sentence of **up to 1 year** (KZ-1 §306).
- 4c. Is gaining financial gain through misuse of computers - **up to 5 years** (KZ-1, §237) and money laundering - **5-8 years** (KZ-1, §252).

ATT. VEC. 3. Exploit family – exploit 2 (blackmail)

1. Janja (we have her mail and business address) receives an email from an unknown source.
2. 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.
3. 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.
4. The email contains a payload, something like: emotet[1], formerly banking malware that analyses the targets inbox, learns their writing style and phishes on.

[1]https://www.malwarebytes.com/emotet/
https://www.fortinet.com/blog/threat-research/analysis-of-a-fresh-variant-of-the-emotet-malware.html

ATT. VEC. 3. Exploit family – exploit 2 (blackmail)

- Blackmail / extortion (3) carries a jail sentence of up to **5 years** a pop (KZ-1 §213).
- (4) is an unauthorized intrusion into a computer system, which carries a jail sentence of **1-5 years** (KZ-1, §221 or §237).
- Possession of hacking tools carries a jail sentence of **up to 1 year** (KZ-1 §306).
- (3) Is gaining financial gain through misuse of computers - **up to 5 years** (KZ-1, §237) and money laundering - **5-8 years** (KZ-1, §252).

ATTACK VECTOR 4. the Next step

1. In steps 1 – 3 we get access to someone's inbox. Either Janja's or Oliver's.
2. We look at the emails, writing style, upcoming events, ongoing conversations…
3. The interim goal is Oliver. The final destination is Barbara Domicelj.
4. 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.
5. If Oliver never, ever, writes to Barbara, we look through Oliver's mailbox and find someone who connects Oliver and Barbara. We exploit them.
6. There are always ways to circumvent mechanical protection! Kieren and I observed our trainees circumvent them *again and again and again*, using social engineering.

ATTACK VECTOR 5. Viable attacks

Viable attack 1. Transfer funds

- Check Barbara's computer. Look whom she corresponds with. Does she talk to Microsoft management? How does she approve purchases. Who dose she talk to? When is she away? What are her hobbies?

1. Wait for Barbara to be **away** (Either cf. emails or phone them up).
2. Send an email in her name to the accounting office. Require a large invoice be paid "today!" into an online bank account. Then transferred to Russia / China etc. (I've witnessed this IRL at Cambridge!)

Future talks

- In the future talks, we will explore which psychological mechanisms play a role in security interactions and why.
- You will also learn how to write proper OSINT reports.
- **I still need a volunteer for the Shodan lecture!**

Homework III.

- Send it to me by Monday November 16th 12:00. Best if you submit through Učilnica.
- Gather as much **OSINT information** as you can on **SavaRe postinsurance group**.
- **Absolutely no active measures, not even nmap. They do know they are being probed. Send me a report, provide screenshots and url's. At no point, break the law.**
- No HUMINT! No breaches of physical security. If you insist, you can do physical observation but do not enter MS premises. If you find passwords, let me know, I'll contact SavaRe.
- **If the CTO of Sava calls me and lets me know you have been detected, I will fail you. If malicious, I will kick you off the course and let the CTO know who to prosecute. Do not mess this up.**
- **If in doubt, consult me first.** You have a fortnight.

Next time…

- In a week, Metasploit and Shodan.
- See you then.