Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Ali v informacijski varnosti umetna inteligenca potolče človeško?

22.10.2019

doc. dr. David Modic

AKADEMIJA Finance

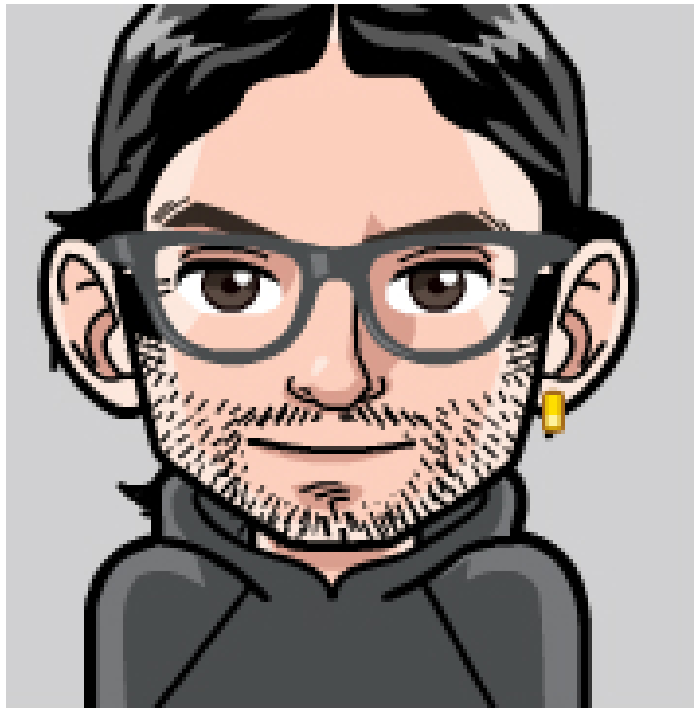
Potek

- Kdo, kaj, kje.
- Na splošno o vdorih.
- Modeli groženj.
- Praktičen primer.
- Odzivanje na napade.
- Vloga umetne inteligence.

- *N.B.* ***(ANKETA)***

david@crq.systems

Kdo, kaj in kje



- doc. dr. David Modic, ekonomski psiholog.
- gostujoči učitelj (docent) in raziskovalec na FRI, UL.
- starejši član King's College, Cambridge.
- pred FRI:
  - raziskovalec, Univerza v Cambridgeu, računalniški laboratorij
  - bivši namestnik direktorja CamCERT (socialni inženiring)
  - gostujoči akademik, Univerza v Cambridgeu, Inštitut za kriminologijo
  - častni član Univerze v Exetru, VB (2012–2017)
- svetovalec (UIS, brazilska vlada, podjetja, britanska vlada, NATO).

- Kaj počnem: *raziskujem kiber kriminal in psihologijo računalniške varnosti, izvajam penetracijska testiranja, hekerske maratone, šolanja in testiranje podjetij.*

https://david.deception.org.uk

david@crq.systems

Odgovor na prvotno vprašanje!

- Ali v informacijski varnosti umetna inteligenca potolče človeško?
  - Po mojem ne.
  - A gremo domov?
- Ali naj raje ponudim malo daljši odgovor?
- V tem primeru pojdimo na začetek.

O vdorih na splošno

- **(ANKETA) Ali je poskusov vdorov vedno več?**
  - Poročila o vdorih pravijo, da ne. Kako bi jih sploh lahko bilo več? *[ENA UNIVERZA]* denimo je v povprečju napadena vsakih 13 sekund. Bi kdo opazil razliko?
- **(ANKETA) Ali napadalci uporabljajo vedno nove prijeme?**
  - Ja in Ne. Kot pravi Djodje Balašević: „*Princip je isti, sve su ostalo nijanse.*“

Najhujši napadi?

- Kaj mislite, kateri so najhujši?
- **(ANKETA) So najhujši napadi tisti, ki**:
  - Ogrozijo državno infrastrukturo (npr. *notPetya* v Ukrajini. Tudi v Sloveniji najdemo luknje v državni infrastrukturi, vendar o njih ne bom govoril)?
  - Spremenijo družbeno ureditev (*Brexit* ali *ameriške predsedniške volitve*)?
  - Uničijo sloves podjetja (npr. *[ENO PODJETJE]*)?
  - Poberejo ves denar ovdoveli babici in jo spravijo na cesto?
- Po mojem je edini smiseln odgovor na to vprašanje: *„Najhujši so tisti napadi, ki se zgodijo nam.“*

Katerih napadov je največ?

- Največ napadov je mehanskih. *50x na sekundo poskus dostopa do komandne vrstice. 5.000.000 simultanih dostopov do strežnika z namenom onemogočanja storitve (DDOS).*
- **(ANKETA) So tisti, ki so najbolj pogosti tudi najbolj učinkoviti?**
  - NE! Najbolj učinkoviti so tisti, ki so narejeni po meri.

Na koliko napadov se napadeni obranijo?

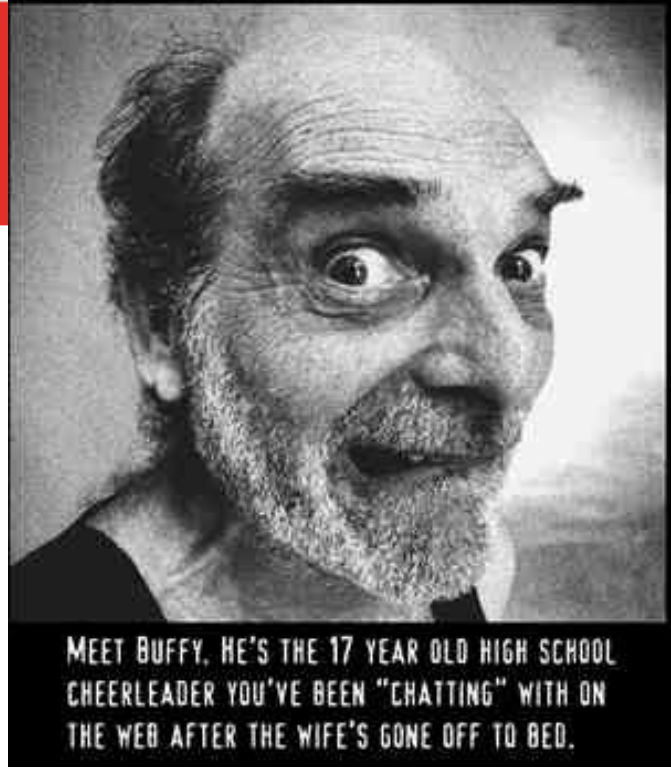
- Suhoparno gledano se npr. *[ENA UNIVERZA]* obrani približno 99.25% procentov napadov. Večine jih sploh ne zaznamo. *Če imamo infrastrukturo urejeno.*
- Če vprašanje obrnemo, torej, *koliko napadov je uspešnih*, pa naletimo na ogromne metodološke težave.
  - Nihče pri zdravi pameti nenadzorovano ne poroča javnosti o vdoru.
  - Tisti, ki vemo za uspešne napade, bi po navadi radi še kdaj kaj počeli.
  - Če bi obstajal portal, ki bi objavljal podatke o uspešnih napadih, bi ga črni klobuki obiskovali in osveževali brez prestanka.

Groba delitev vdorov / napadov.

- Vdore bi lahko na grobo delili na tiste, **(a)** ki izrabljajo **naprave** in tiste, **(b)** ki izrabljajo **ljudi**.
- **(ANKETA) Katerih je več?**
  - Tistih, ki izrabljajo naprave.
- **(ANKETA) Kateri so bolj uspešni?**
  - Tisti, ki izrabljajo ljudi.

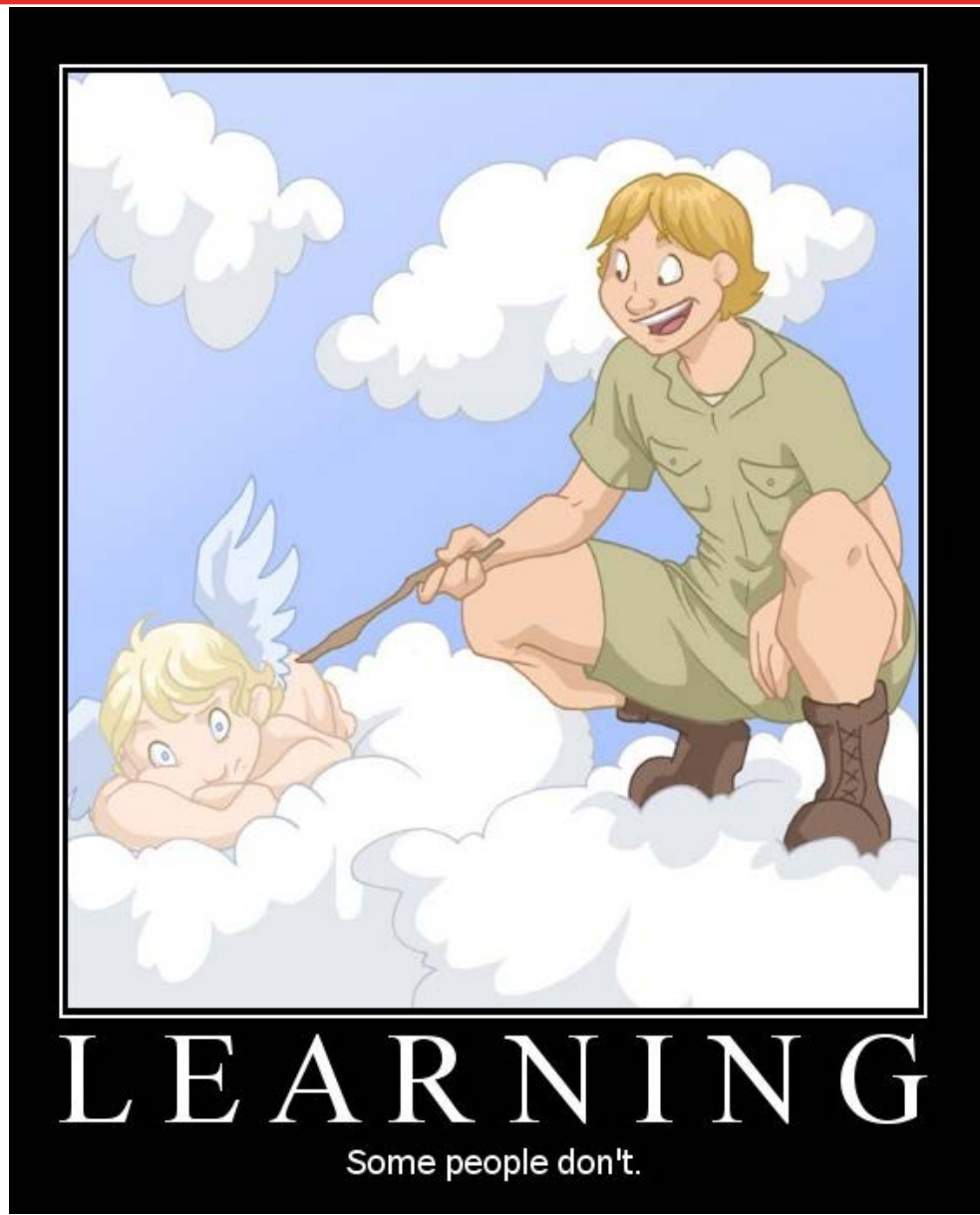
Zakaj napadi na človeške vire?

- **(ANKETA) Kaj mislite, zakaj napadi na človeške vire?**
  - Ker so bolj poceni.
  - Ker zahtevajo manj predznanja.
  - Ker so bolj učinkoviti.
  - Ker obramba misli, da so vsi enaki kot oni (*primer mojih študentov*).
  - Ker dosega cilje modela grožnje (*primer okrogle mize o varnosti*).



Iz primerov se najlaže naučimo

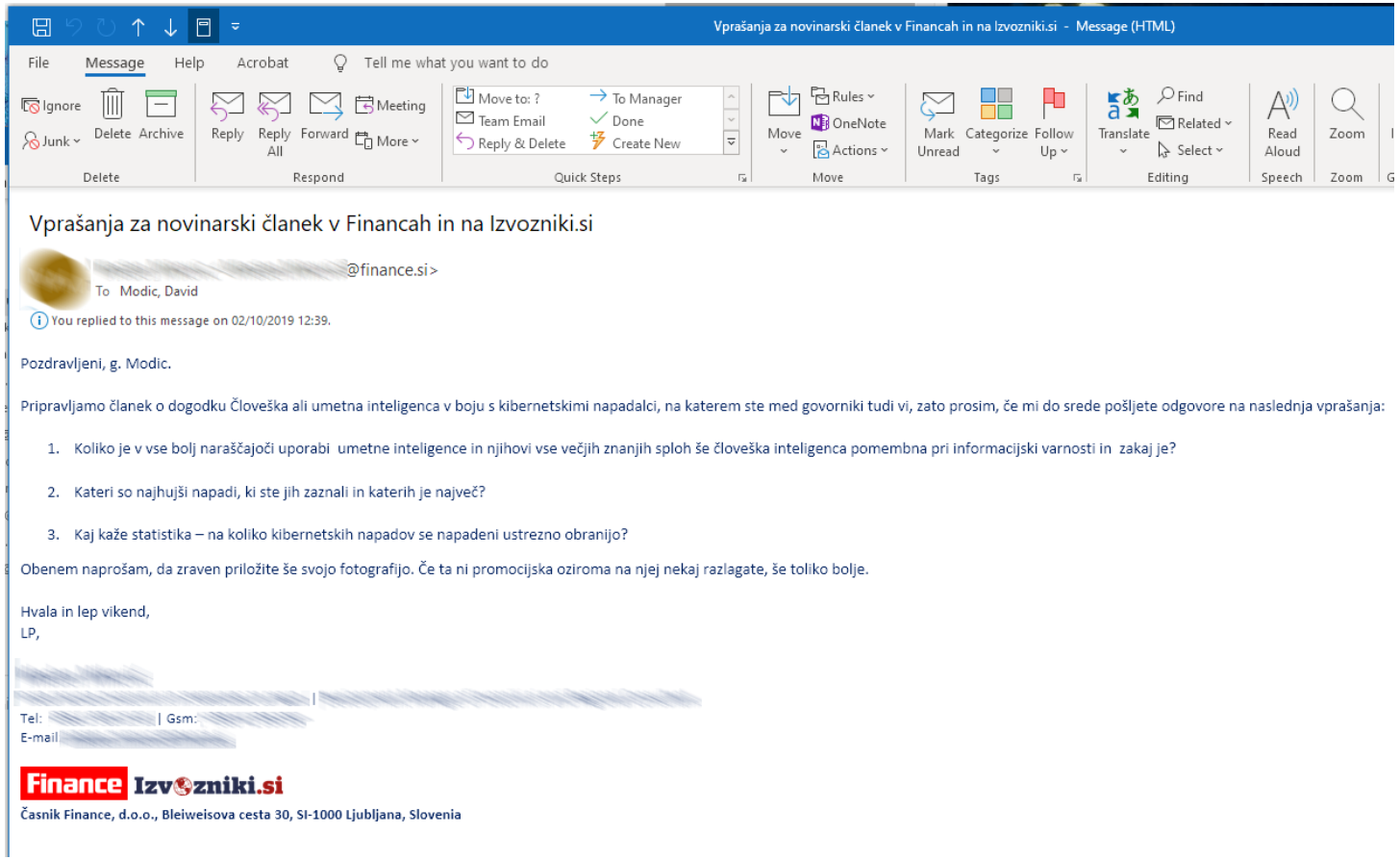
- Ker smo ravno na konferenci, ki jo organizirajo Finance in sponzorira A1, si izberimo priročno tarčo.
- Katerokoli od obeh podjetij bi mi ustrezalo.
- Dokler nisem dobil prošnje za intervju (ki mi je služila kot odskočna deska).



david@crq.systems

Prošnja

- Tri vprašanja:
  - Umetna inteligenca in varnost (s podtonom – *AI YAY! Ljudje BUU!*).
  - Najhujši in najbolj pogosti napadi?
  - Koliko podjetij se uspešno obrani?
- Prošnja za fotografijo.



Vprašanja za novinarski članek v Financah in na Izvozniki.si - Message (HTML)

File Message Help Acrobat Tell me what you want to do

Ignore Junk Delete Archive | Reply Reply All Forward Meeting More | Move to: ? Team Email Reply & Delete To Manager Done Create New | Move Rules OneNote Actions | Mark Unread Categorize Follow Up | Translate Find Related Select | Read Aloud | Zoom

Delete Respond Quick Steps Move Tags Editing Speech Zoom

Vprašanja za novinarski članek v Financah in na Izvozniki.si

[redacted]@finance.si>

To Modic, David

You replied to this message on 02/10/2019 12:39.

Pozdravljeni, g. Modic.

Pripravljamo članek o dogodku Človeška ali umetna inteligenca v boju s kibernetskimi napadalci, na katerem ste med govorniki tudi vi, zato prosim, če mi do srede pošljete odgovore na naslednja vprašanja:

1. Koliko je v vse bolj naraščajoči uporabi umetne inteligence in njihovi vse večjih znanjih sploh še človeška inteligenca pomembna pri informacijski varnosti in zakaj je?
2. Kateri so najhujši napadi, ki ste jih zaznali in katerih je največ?
3. Kaj kaže statistika – na koliko kibernetskih napadov se napadeni ustrezno obranijo?

Obenem naprošam, da zraven priložite še svojo fotografijo. Če ta ni promocijska oziroma na njej nekaj razlagate, še toliko bolje.

Hvala in lep vikend,
LP,

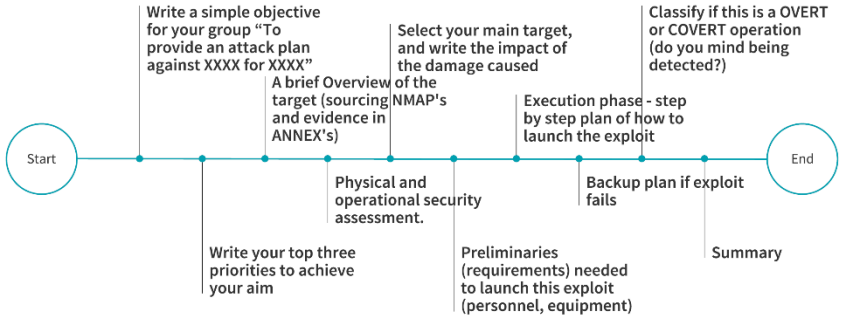
[redacted]

Tel: [redacted] | Gsm: [redacted]
E-mail [redacted]

Finance Izvozniki.si

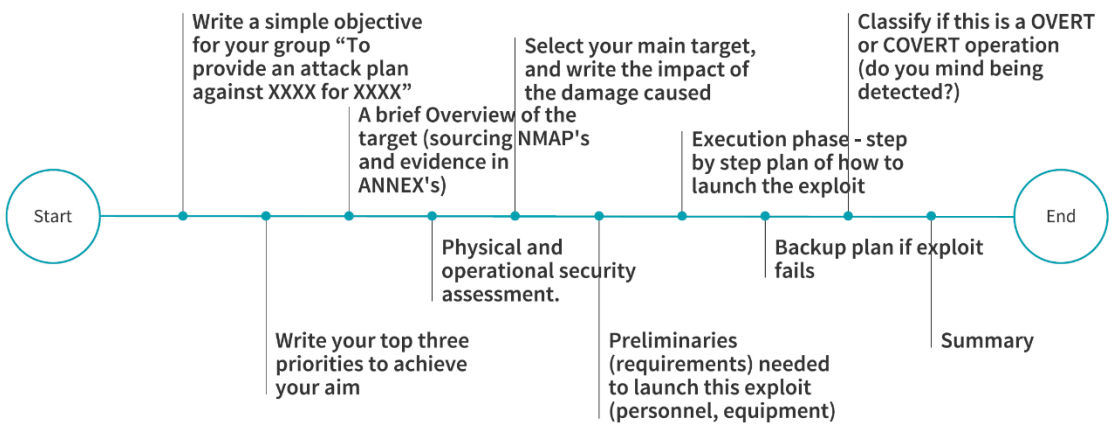
Časnik Finance, d.o.o., Bleiweisova cesta 30, SI-1000 Ljubljana, Slovenia

Tipičen primer napada

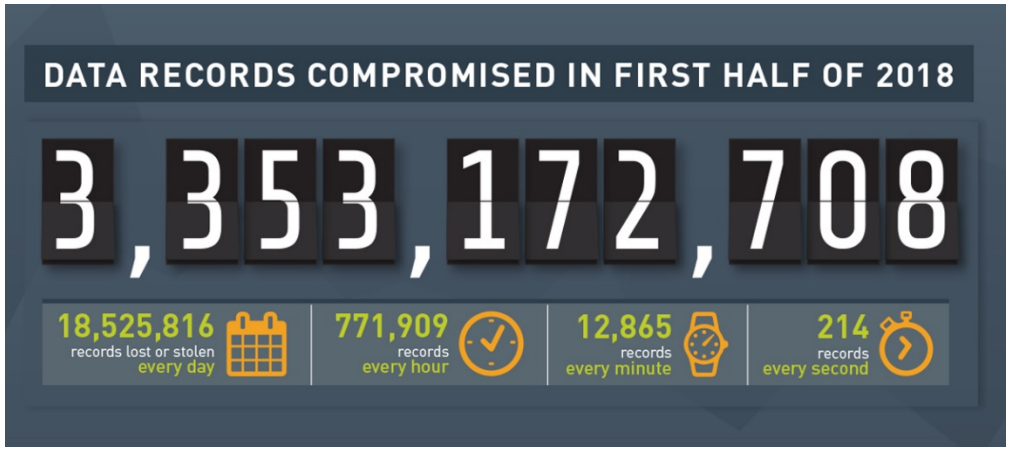


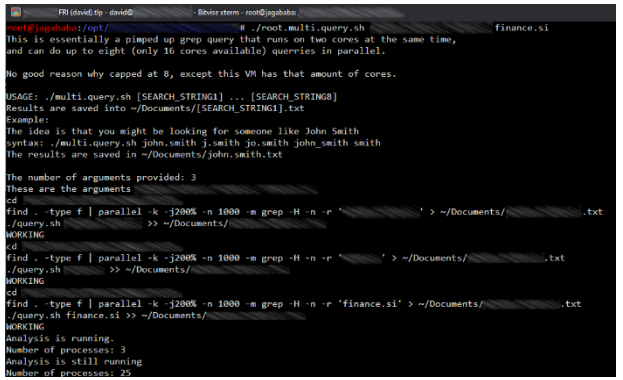
- Uspešni napadi bodo:
  - Potekali po več vektorjih naenkrat (primer Locked Shields 2019).
  - Indirektni (tudi če je cilj direktor, ne napadeš direktorja).
  - Vsebovali pred-pripravo (OSINT).
  - Oblikovani po meri.
  - Vsebovali jasno izoblikovan model grožnje in omilitvene dejavnike.

OSINT



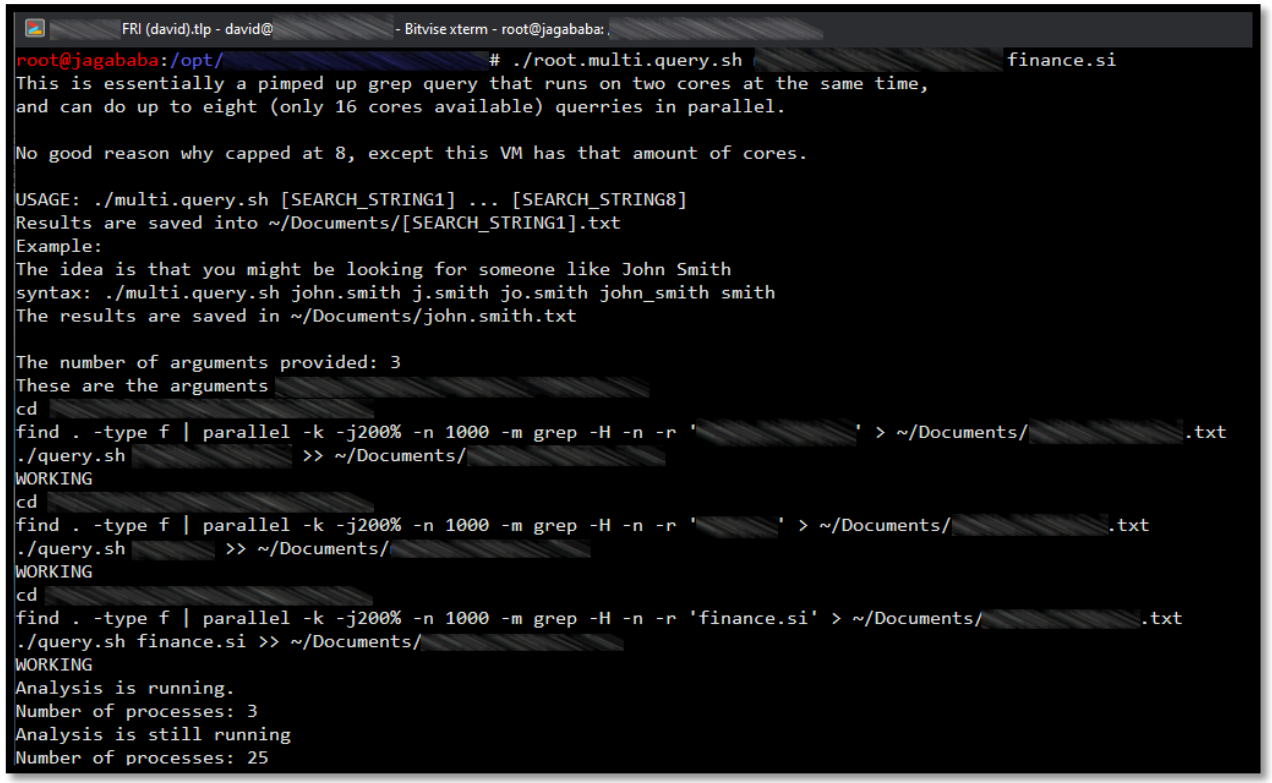
- V tem primeru nisem zbral praktično nobenih informacij javnega značaja. Ni bilo potrebe.
- Edina stvar, ki sem jo naredil je, da sem pogledal, če so Finance.si zabeležene v bazi vdorov.
- Vsi vemo kaj so baze vdorov?





Finance.si (baza vdorov)

- Finance so prisotne v moji bazi.
- Ne trdim, da so to službena gesla.
- Mnoga so verjetno že zamenjana.
- Na splošno lahko rečemo tole:
  - NITI GESLO ENO NI MOČNO.
  - Vsa so devet ali manj znakov.
  - Niti eno ne vsebuje posebnih znakov.
  - Imena otrok in partnerjev.
  - Slovarske besede.
  - Ime in letnica rojstva.
  - Eno geslo je samo številka.
  - Eno geslo je ponovljen e-mail.
  - Eno je, dobesedno, *Password123*



Baza vdorov - pomisleki

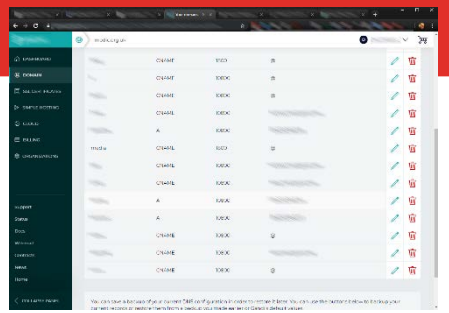
- Je moralno sporno, da razkrivam podatke iz baze?
  - Nisem edini, ki ima dostop do takih podatkov.
  - Če imam dostop jaz, ga imajo tudi črni klobuki.
  - Posredno imajo dostop do vaših gesel (če ste v bazi).
  - Imeli so ga dosti pred tem predavanjem.
  - Gesel nisem objavil, samo opisal sem jih. Tisti, ki se najdejo v mojih opisih, pa bi gesla tako ali tako že zdavnaj morali menjati.

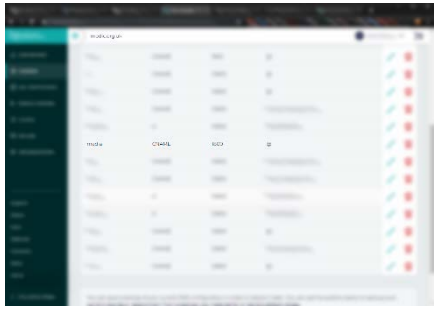
Moj "napad"

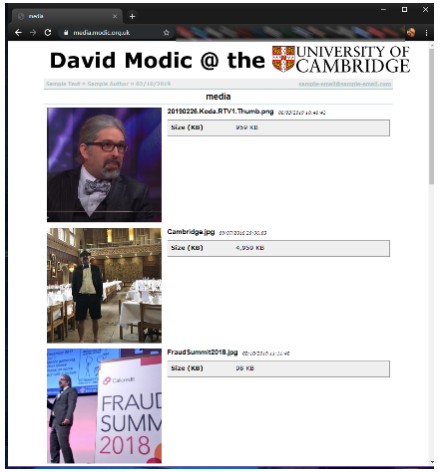
- Uporabljam samo javno dostopne informacije.
- Dva vektorja napada:
  1. Povsem nediskriminatoren (usmerjen proti celotnim financam.si). *Že uspešno opravljen.*
  2. Bolj usmerjen.
- Najprej pred-priprave.

Prep

- Ustvarim si dns zapis. Za *media.modic.org.uk*.
- Pridobim certifikat, da dobim **https://media.modic.org.uk**
- Izdelam spletno stran s svojimi fotografijami in jo objavim.
- Na to spletno stran *bi lahko naložil* t.i. drive-by-malware (programje, ki se naloži, ko obiščete spletno stran). Ampak to bi bilo nezakonito (Posedovanje orodij, ki omogočijo kaznivo dejanje. KZ-1 §306(2). *Do enega leta zapora za vsako orodje*).
- Naložim sledilec in grafični vmesnik za analizo dnevnika (t.i. log analyzer) *goaccess*.

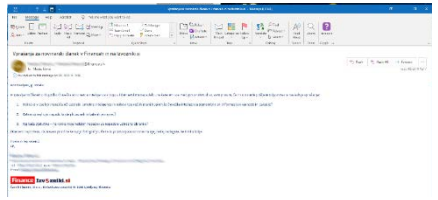


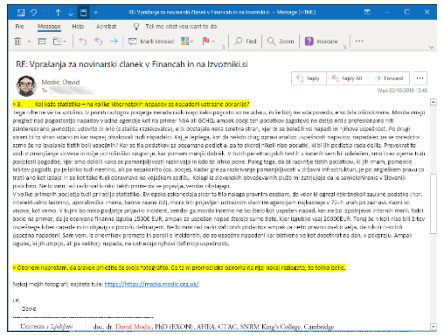


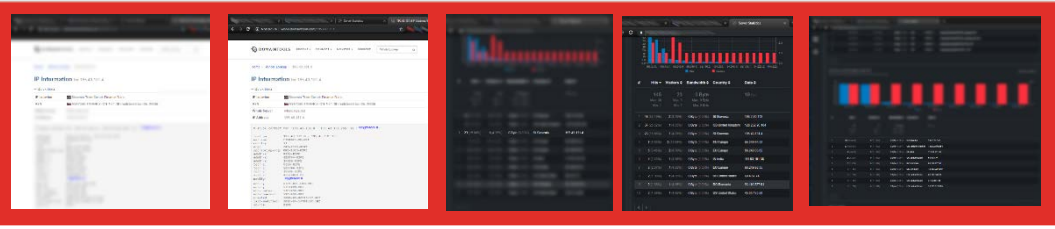


Prep II.

- Novinar mi je poslal pošto. V njej me je prosil, da mu pošljem kako svojo sliko.
- Odgovorim mu, in mu pošljem povezavo na svojo spletno stran s fotografijami. https://media.modic.org.uk.
- *Če obišče spletno stran, bi mu lahko naložil poljubno programje na njegov računalnik. Če dela od doma, potem imam njegovo domačo mrežo. Če iz službe, sem pravkar dobil dostop do interne mreže Financ.*



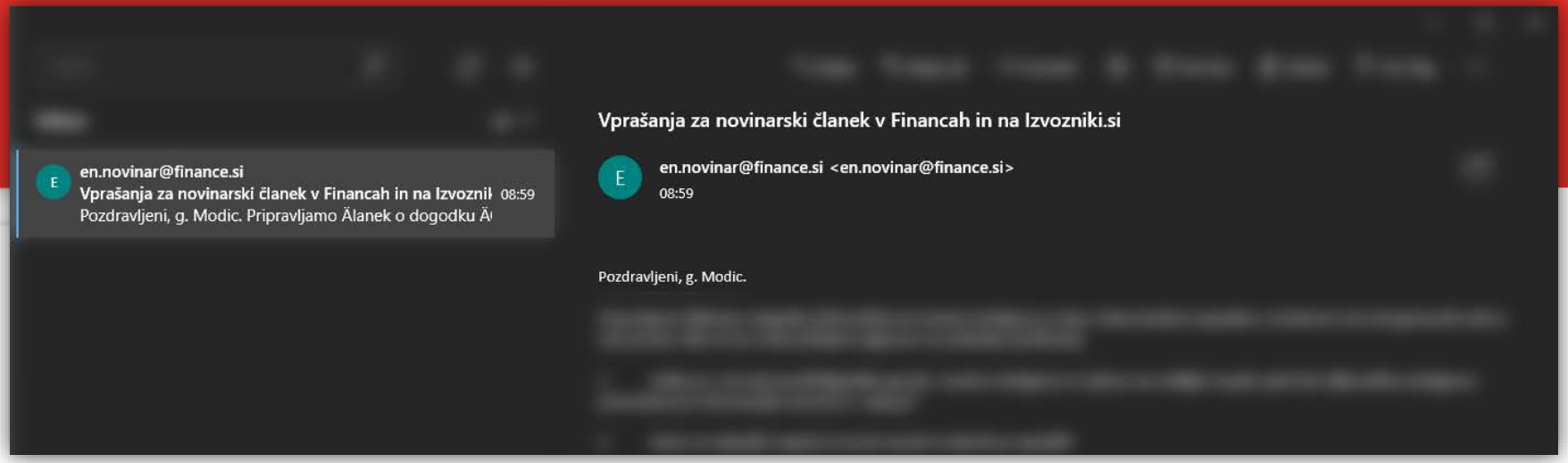




Potek

- *Seveda mora novinar najprej mojo stran obiskati, za uspeh.* Poglejmo dnevnike.
- Prvotni dnevnik (zabeležen pred mojo pošto novinarju), ne kaže nič posebnega. Dostopal sem jaz, pa moj strežnik, pa neki Romuni, Američani in Indijci.
- Par dni kasneje je slika malo drugačna.
- Osredotočim se na IP številko, ki prihaja iz Slovenije ampak ni del naslovnega prostora FRI.
- Bingo! Finance.

Ampak! Ampak!



- … bo rekel nekdo iz publike. „*Saj je on poslal tebi pošto in dobil odgovor od tebe. Kriv je samo tega, da ni računal, da boš ti taka rit, da mu boš poslal zlobno povezavo.*“
- To bi bilo res, če bi on lahko z gotovostjo vedel, da sem pošto poslal jaz. To, da sem jaz na videz “pošiljatelj” ničesar ne dokazuje.

Ok. *Kaj pa to pomeni?*

- Če bi bil napadalec bi imel vsaj dva načina dostopa do interne mreže Financ.
- Od tam bi se lahko razširil na druge računalnike, s končnim ciljem dostopa do (a) finančne službe, (b) lastnikov, (c) uredniške pisarne (za lansiranje lažnih novic).
- **Vsi nadaljnji koraki bi bili ne-etični in nezakoniti**.

O izrabi človeških virov

- Morda se komu od vas zdi novinar neumen. Kako ni vedel, da ga bom *phishal*?
- Ni pomislil, ker nihče od nas ne bi, razen tistih s paranoidnimi blodnjami ☺.
- Ohraniti OPSEC je *težko*.
- Moj cilj nikakor ni, da bi sramotil novinarja. Verjemite mi, da bi praktično vsi v tej sobi reagirali enako (*primer prepisovanja URLjev v zadnjem pen testu, ki smo ga izvajali*).

(a) Če bi v resnici napadal, potem bi najprej poslal pošto s paketom kar nekam na finance (npr. na info@finance.si), da bi videl, če mi jo zavrne.

(b) V pošti, bi opozoril, da je "format slik" tak, da rabi poseben gonilnik za odpiranje (kar ni del operacijskega sistema), in da se bo avtomatično naložil. Če ne bo nobenih opozoril, pa toliko bolje.

Zakaj sploh govorim o tem?

- Ker ne poznam ekspertnega sistema, ki bi preprečil tak vdor.
- IDS ga verjetno ne bi zaznal.
- Vsi opisani postopki so vsakdanji. (*Pošlješ pošto, jo dobiš nazaj*…).
- Ker je povezava s strežnikom zakodirana zlonamerne kode večina požarnih zidov / IDS ne bi zaznala. Možno je, da bi se uprl namizni računalnik, ampak tudi to se da zaobiti.
- Pa smo pri umetni inteligenci in varnosti.

Koristnost mehanskih rešitev?

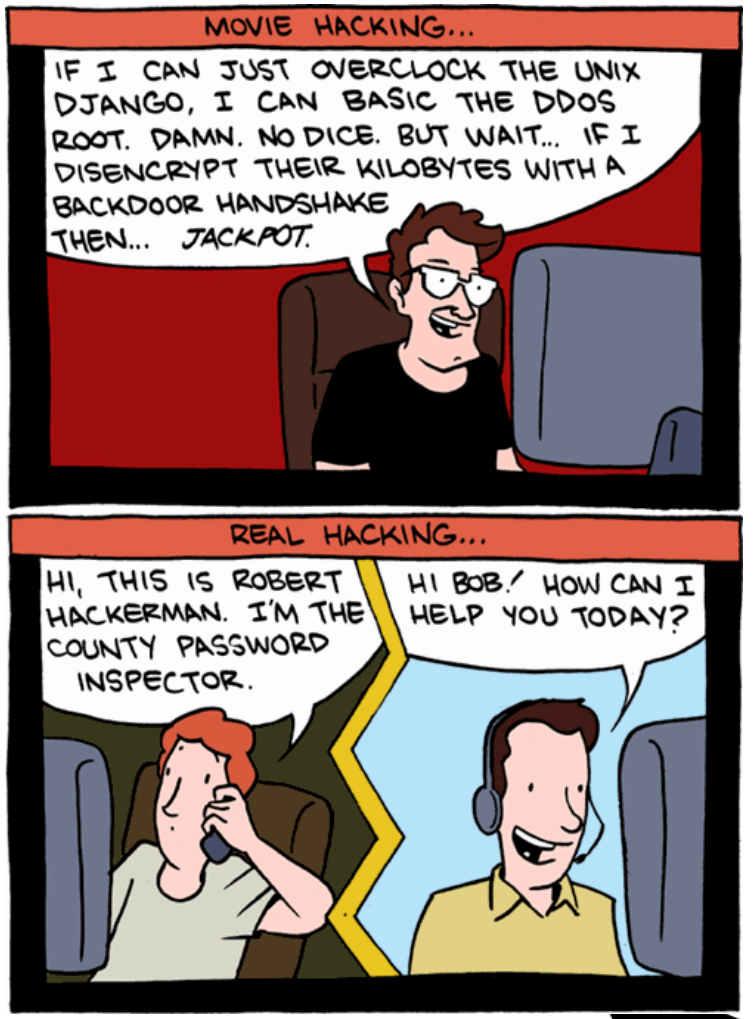
- Mehanske rešitve so nujne, ker zaznajo večino napadov.
- Umetna inteligenca prepozna običajne vzorce napadov.
- Svetujem vam uporabo obstoječih rešitev. Sistemski administratorji vam bodo hvaležni.
- Oboje (AI + IDS) pa ni dovolj pri dveh tipih napadalcev:
  a) Tistih, ki so si izbrali ravno vas in oblikujejo napad po meri.
  b) Tistih, ki jih sponzorira kaka država, oziroma so zaposleni v kaki državni obveščevalni službi.

Kaj torej narediti?

- Rabite SOC, kjer so zaposleni ljudje, ki razumejo varnost.
- Bolje, da imate svojega.
- Če to ni smiselno ali je predrago, potem izberite takega, kjer zaposleni razumejo tudi človeško dimenzijo napadov.

Ali umetna inteligenca potolče človeško v INFOSEC?

- V hitrosti odzivanja, **ja**.
- V prepoznavanju običajnih vzorcev napadov, **ja**.
- V prepoznavanju napadov narejenih po meri, **ne**.
- V razvijanju novih obrambnih sistemov, **ne**.
- V obvladovanju javnosti in komuniciranju o napadih, **ne**.



david@crq.systems

Hvala za pozornost!

Vprašanja?

david@crq.systems


Univerza v Ljubljani
Fakulteta za računalništvo
in informatiko
www.fri.uni-lj.si
www.facebook.com/ulfri