



En hackers historie

Tar robotene over?

Av Daniel Christensen (Pentester/Etisk hacker I Telenor)

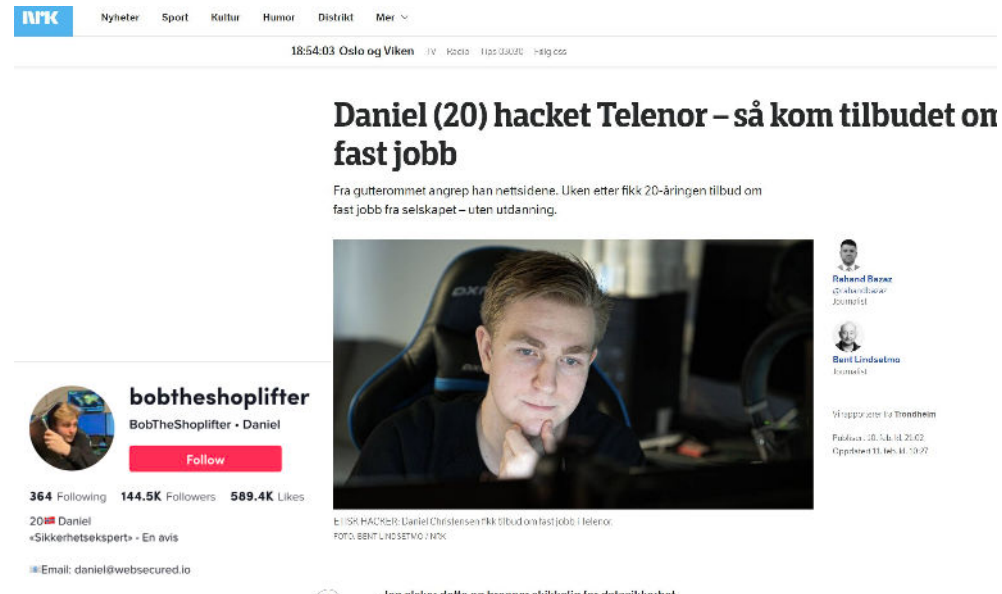


Hvem er jeg?



Hvem er jeg?

- 21 år, programmerer og etisk hacker
- IKT Servicefag på VGS
- Hacka meg til fast jobb i Telenor
- Norges største IT Tiktoker



Daniel (20) hacket Telenor – så kom tilbudet om fast jobb

Fra gutterommet angrep han nettsidene. Uken etter fikk 20-åringen tilbud om fast jobb fra selskapet – uten utdanning.

bobtheshoplifter
BobTheShoplifter • Daniel
364 Following 144.5K Followers 589.4K Likes
20 Daniel
«Sikkerhetsekspert» - En avis
Email: daniel@websecured.io

Rehnd Bævre
Journalist

Bent Lindalmo
Journalist

Stappstøtte fra Trondheim
Publisert 10. feb. kl. 20:02
Oppdatert 11. feb. kl. 19:27

151 HACKER: Daniel Christensen fikk tilbud om fast jobb i Telenor.
Foto: BENT LINDALMO / NRK

...len elsker dette og brenner skikkelig for datasikkerhet.

Heil

Dette ser virkelig ikke bra ut, jeg skal sørge for at det blir tatt tak i internt. Du kan fint forsøke å sende det over på mail.

Kjenner ikke deg og din profil, men har du sett at vi søker etter sikkerhetskompetanse? :-)
<https://www.telenor.no/om/jobbitelenor/ledige-sikkerhetsjobber-i-telenor/>

Takk for innsatsen!

Mvh,
Kristine
Telenor SOC



Hva gjør jeg?

- Pentesting
- Scanner Norge
- 450k .no domener
- 1,500,000 subdomener
- Hacker så og si alt
- Kjemper for et sikrere Norge!

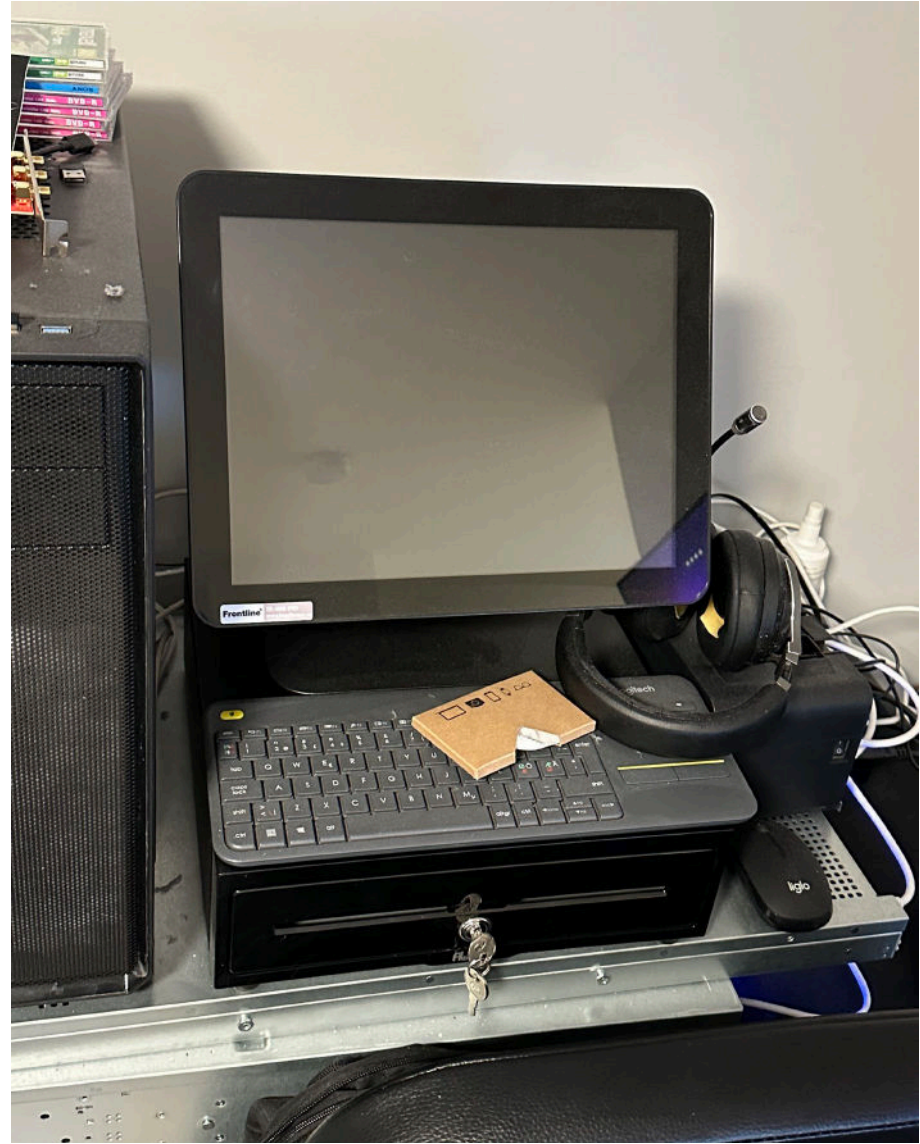
The image shows two screenshots of the MongoDB Compass interface. The top screenshot displays the 'domains.domains' collection with 400.4k documents and 2 indexes. A filter is applied: `{"domain": "nav.no"}`. The document view shows a list of subdomains for the domain "nav.no":

```
_id: ObjectId('6231134b07d3296440f4cf0d')
domain: "nav.no"
subdomains: Array
  0: "fleetdm.gc.nav.no"
  1: "munki.gc.nav.no"
  2: "fs-doc.intern.nav.no"
  3: "metabase.dev.intern.nav.no"
  4: "metabase.intern.nav.no"
  5: "hops.dev.intern.nav.no"
  6: "sentry-dev.gc.nav.no"
  7: "sentry.gc.nav.no"
  8: "api-gw-q.nav.no"
  9: "api-gw.nav.no"
```

The bottom screenshot shows an aggregation pipeline with a filter: `{ field: 'value' }`. The document view shows the result of the aggregation:

```
_id: null
total_sum: 1050848
```





2

Hva er hacking

Og hva er omfanget?



Hva er **hacking**?

- Mr. Robot
- Bryte seg inn
- Få et system til å gjøre noe uventet
- Også fysisk og psykisk (Sosial manipulering)
- Finne veier rundt beskyttende mekanismer

```
.dxxxxx  Ld0MMMMMMMMMMMMddd.  .dxxxxx
.dxxxxx  ,cNMMN,cMMMMx'  .dxxxxx
.dxxxxx  lK;dMMN,cMM0;0k.  .dxxxxx
.dxxxxx  ;Mc .lx.ro, K1  .dxxxxx
.dxxxxxdl;  .  .dxxxxx
.dxxxxx  .:ox  .dxxxxx
.'tox  .dxxxxx

ExploitBox.io

WordPress Core - Unauthenticated RCE Exploit
-----
Discovered & Coded By
David Golunski
https://legalhackers.com
-----
"With Great Power Comes Great Responsibility"
* For testing purposes only *

[*] Sure you want to get a shell on the target 'http://51.13.115.13:8080'? [y/N] y
[*] Guess I can't argue with that... Let's get started...
[*] Connected to the target
[*] Payload sent successfully
[*] Payload executed!
[*] Waiting for the target to send us a reverse shell...

root@srv5743:~/t-test# ./gowitness-2.3.6-linux-amd64 report serve -
19 Feb 2022 19:15:33 WRN exposing this server to other networks is
19 Feb 2022 19:15:33 INF db path path=gowitness.sqlite3
19 Feb 2022 19:15:33 INF screenshot path path=screenshots
19 Feb 2022 19:15:33 INF server listening address=185.125.168.55:71
eterm##$:BKUW300PS345672: 4 root 0 -20 0 0
eterm##$:BKUW300PS345672: astu -ls ./root/fsociety/ -a
eterm##$:BKUW300PS345672: fsociety00.dat readme.txt
eterm##$:BKUW300PS345672: more readme.txt
----- readme.txt-----

LEAVE ME HERE

eterm##$:BKUW300PS345672: sudo kill 4
eterm##$:BKUW300PS345672: |
```



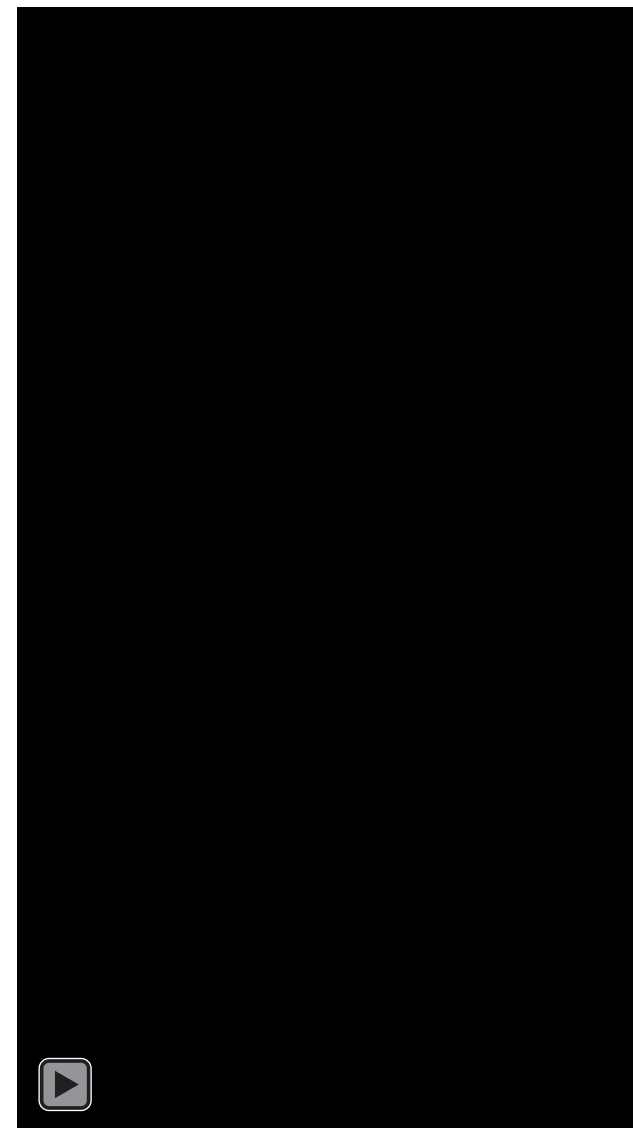


Fysisk sikkerhet er like viktig som digital sikkerhet!

The screenshot displays a mobile application interface for a pizza shop. At the top, there is a receipt titled "Kvittering for ditt kjøp" with order number #612312. Below the receipt is a transaction number: 887666351. The main screen is divided into two panels. The left panel, titled "ORDREBEKREFTELSE", shows a table of items:

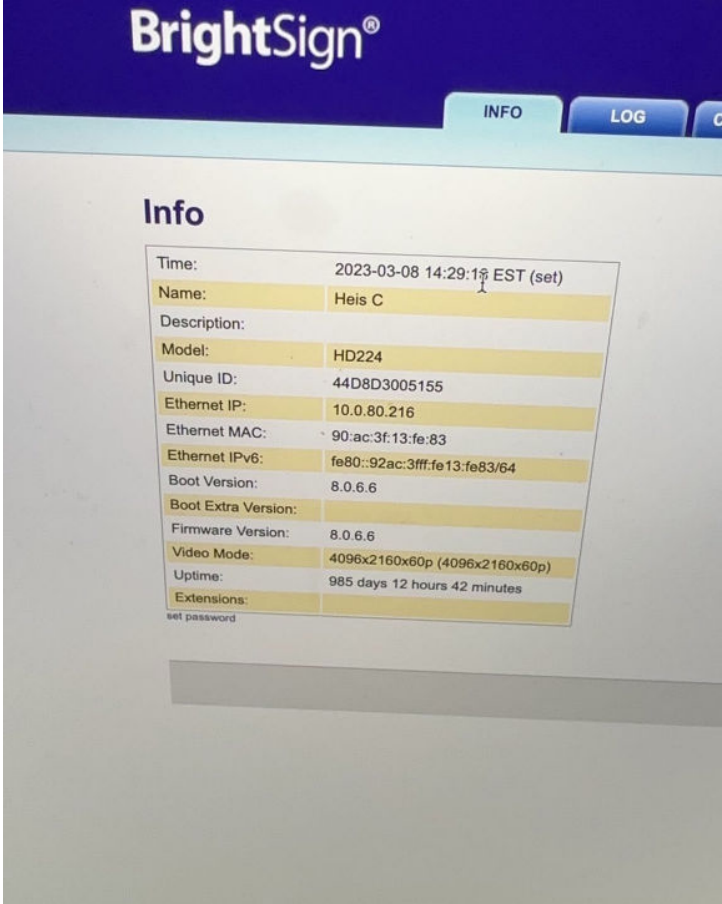
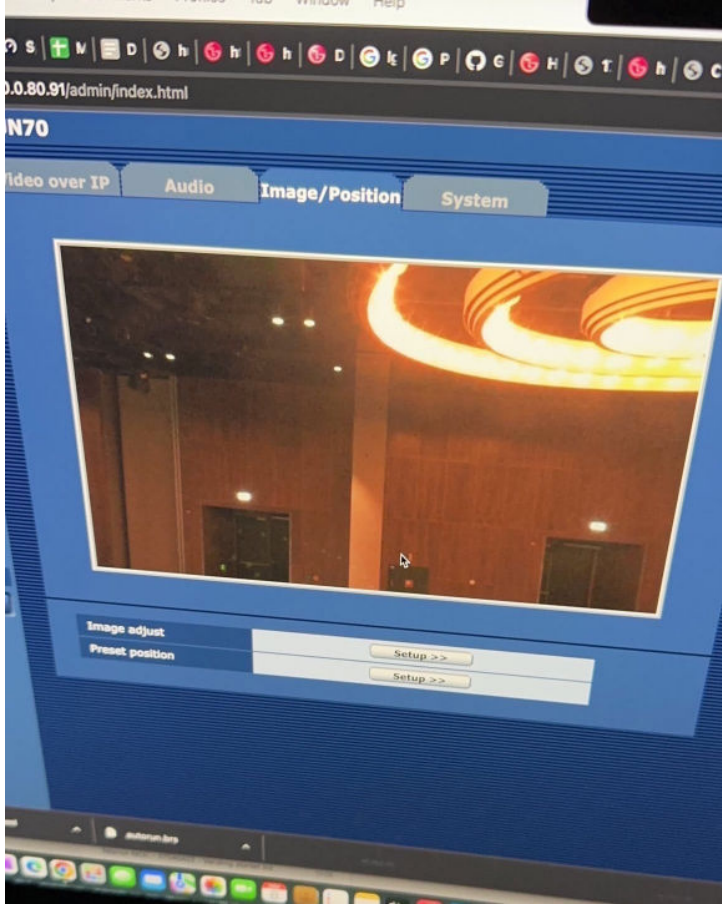
PRODUKT	MENGE	PRIS
SKAP DIN EGEN stor 40,5 cm Amerikansk Free Large (n)	1	kr129,00 kr0,00
Total		kr129,00
Total med rabatt		kr0,00

Below the table is a button "TILBAKE TIL MENYEN". The right panel, titled "DIN KUPONG", contains instructions: "Sett inn ditt produkt i handlekurven og løs inn din kupongkode". It features a "Kupongkode" input field with a green border, a "LØS INN KUPONG" button, and a coupon code "Influencer September". At the top right of the app, there are navigation options: "NO | EN", "PIZZA TRACKER", and a user profile icon. A bottom navigation bar includes "Henting", "Meny", and "Bekreft din bestilling".





Bonus!!



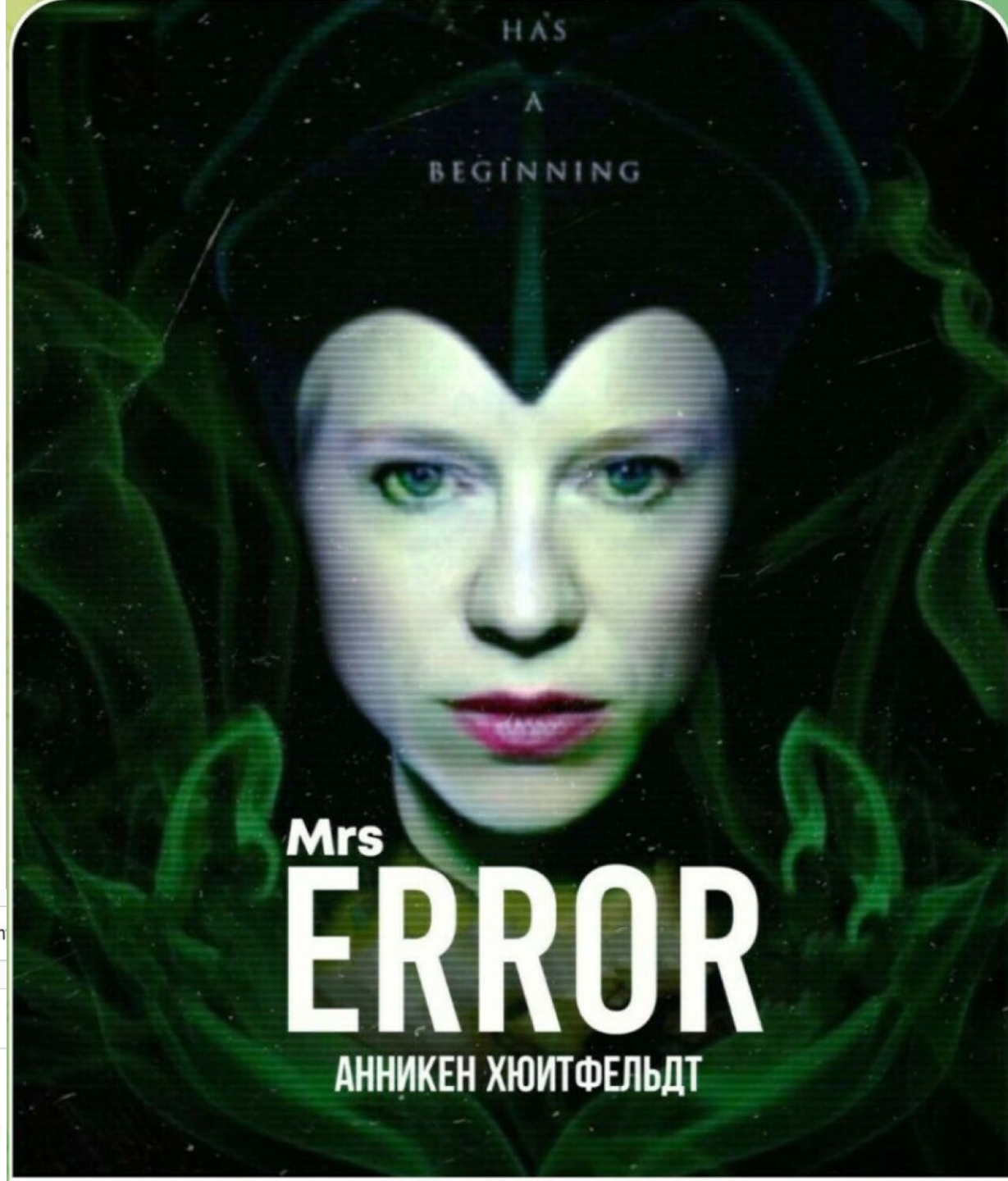
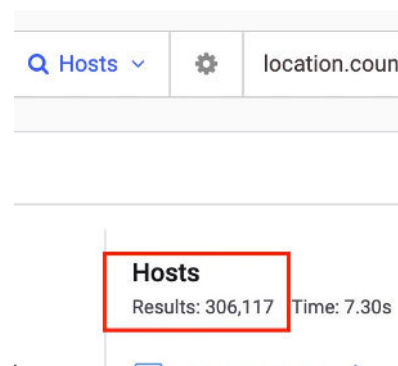
3

Sikkerhet i vår nye digitale verden



Det digitale trusselbildet

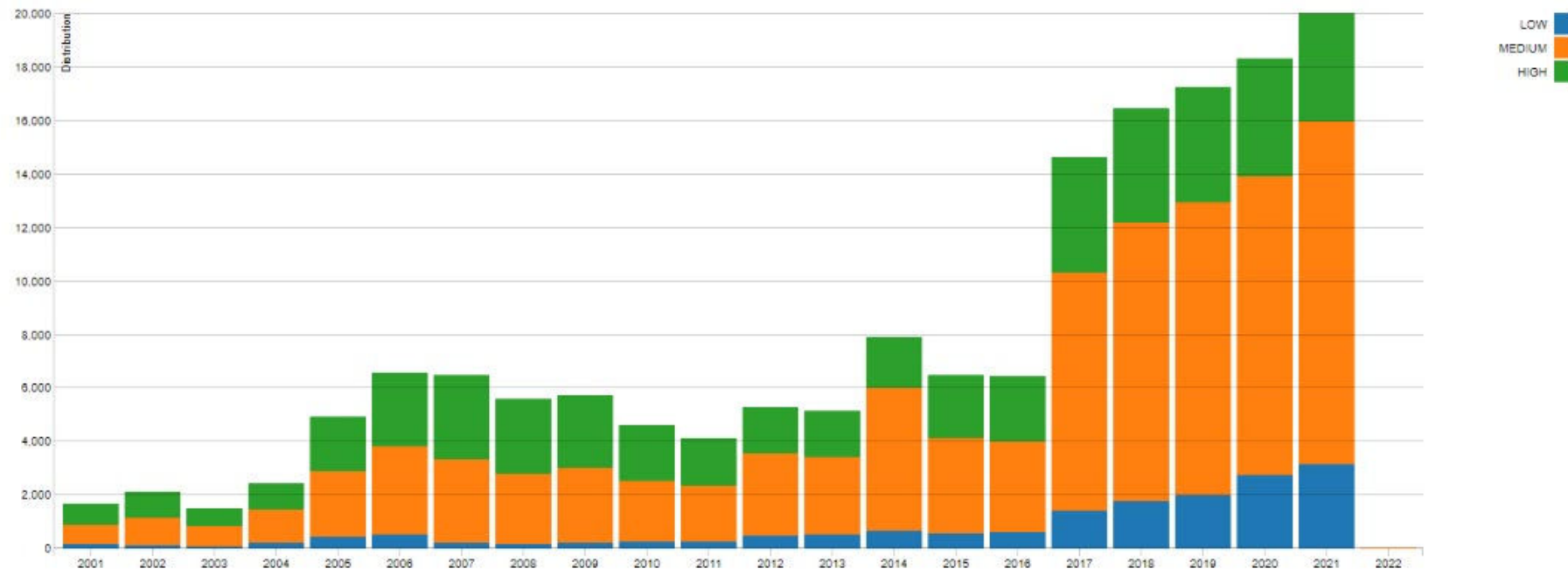
- DDOS hendelsen
- Telco, Helse, Stat og mye mer
- Digital krigføring
- Frykt, propaganda og makt
- Ca 300,000+ estimerte eksponerte maskiner på internett
- IoT (Tunellvifter, Trafikklys)
- Overvåkning
- «Alt er på nett»



Økning i mengden sårbarheter

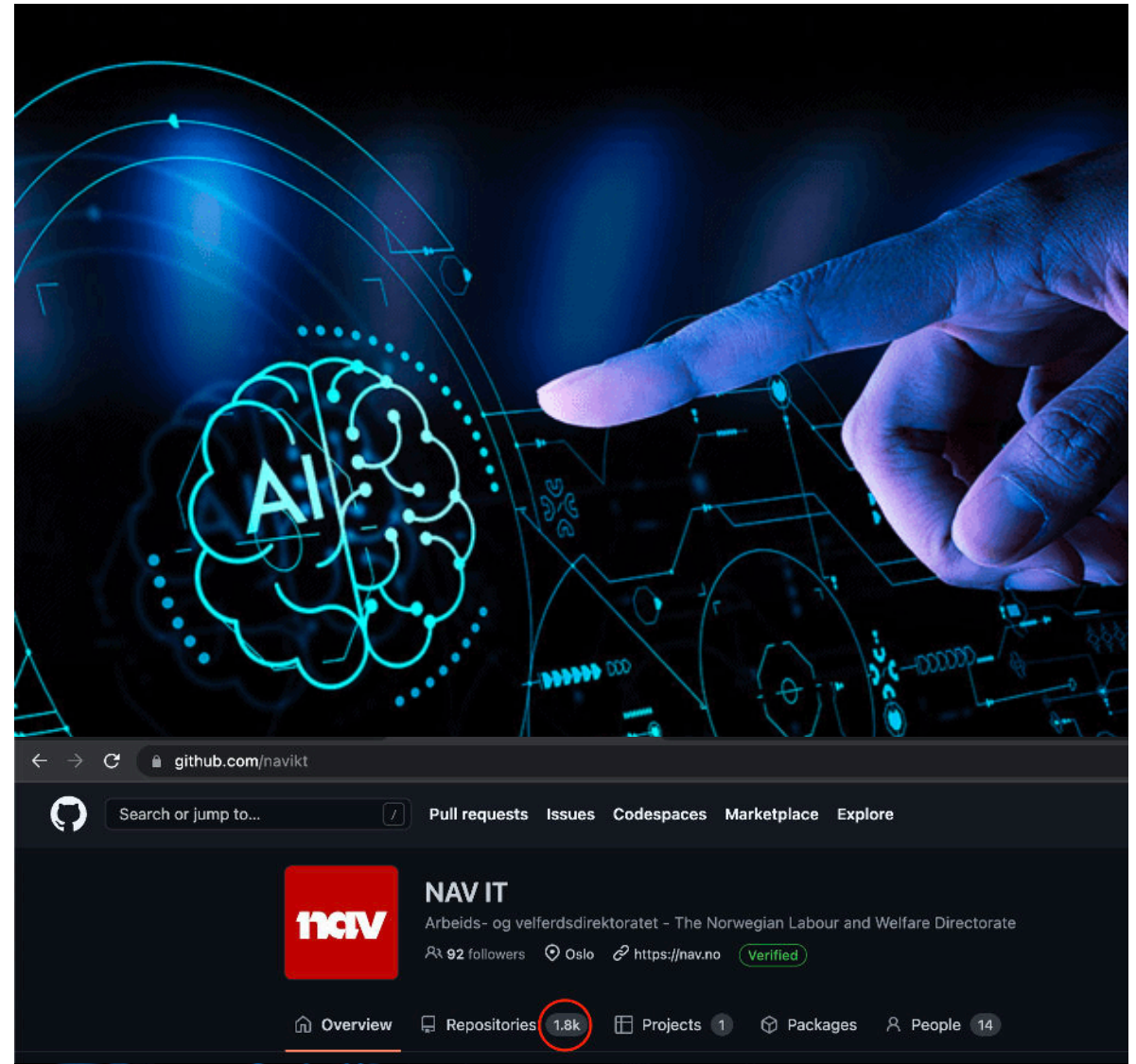
CVSS Severity Distribution Over Time

This visualization is a simple graph which shows the distribution of vulnerabilities by severity over time. The choice of LOW, MEDIUM and HIGH is based upon the CVSS V2 Base score. For more information on how this data was constructed please see the NVD CVSS page .



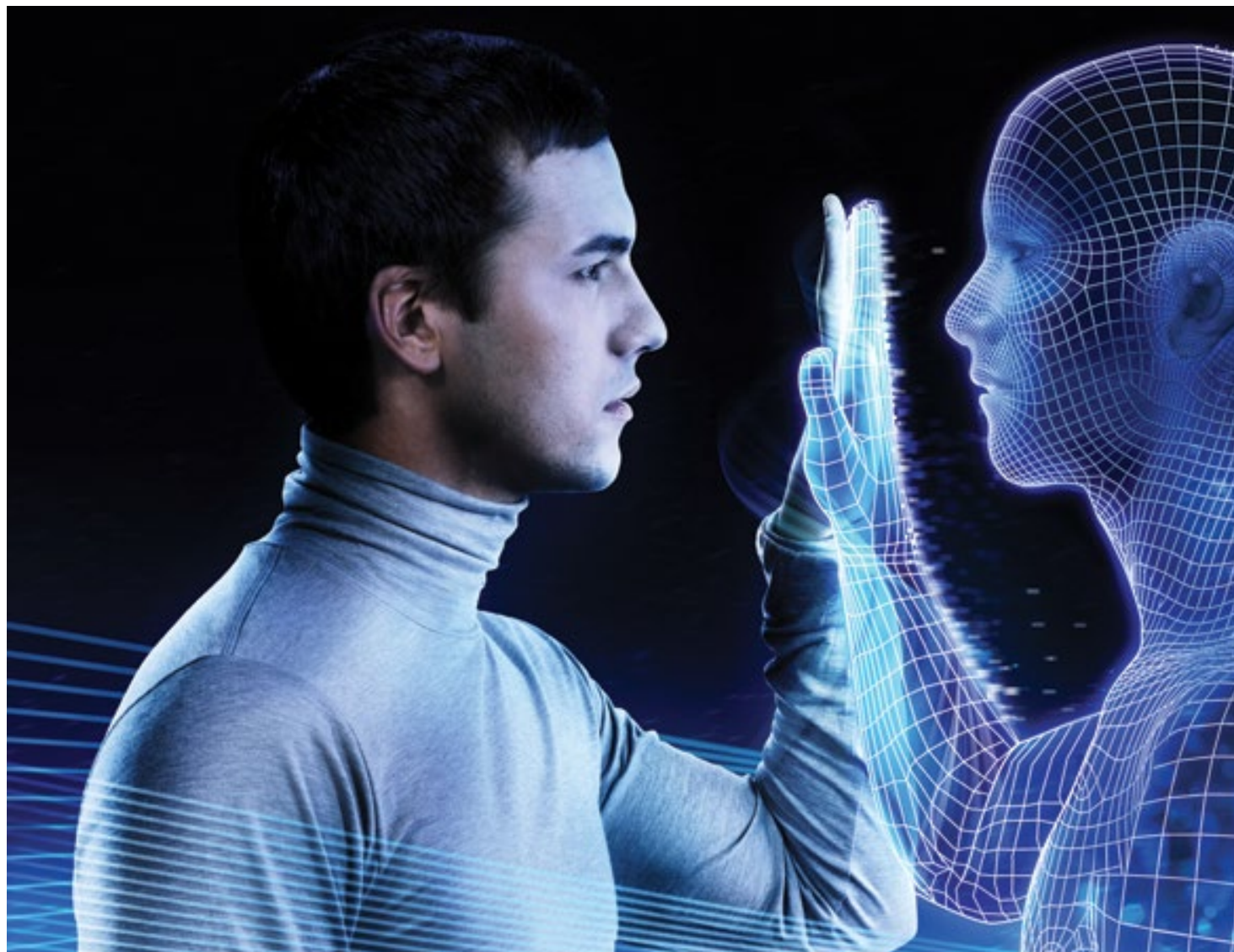
Kunstig intelligens

- Brukes allerede
- Robot mot robot
- Ingen menneskelige behov
- Oppskalering
- OpenAI GPT3
- Åpen kildekode kan skape problemer?



Hva er utfordringene?

- Oversikt
- Digitalisering
- Fysisk sikring
- Lagring av personlig data
- Kryptering i en kvante-maskin verden



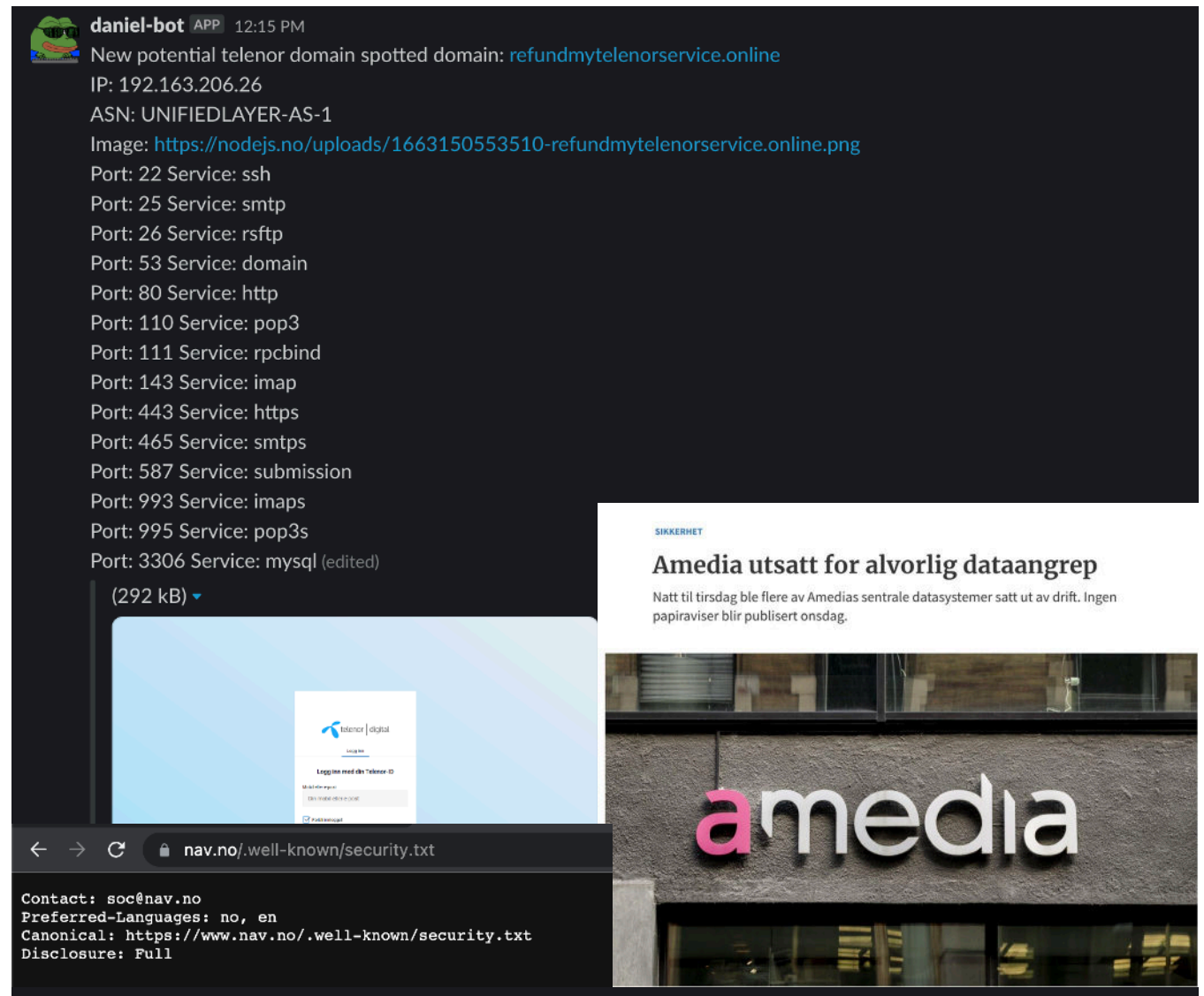


Hva kan vi gjøre nå?



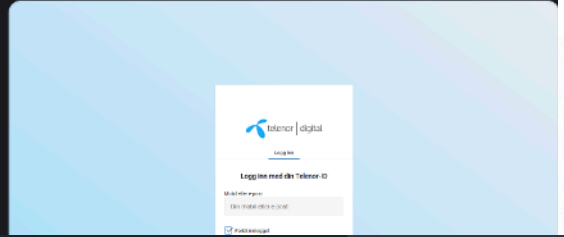
Åpenhet

- Bruke og dele data og angrepsinfo
- Lage nye løsninger
- Vi blir mere åpen om sikkerhet og hendelser
- Bruke kunstig intelligens
- Skape nye arbeidsplasser



daniel-bot APP 12:15 PM
New potential telenor domain spotted domain: refundmytelenorservice.online
IP: 192.163.206.26
ASN: UNIFIEDLAYER-AS-1
Image: <https://nodejs.no/uploads/1663150553510-refundmytelenorservice.online.png>
Port: 22 Service: ssh
Port: 25 Service: smtp
Port: 26 Service: rsftp
Port: 53 Service: domain
Port: 80 Service: http
Port: 110 Service: pop3
Port: 111 Service: rpcbnd
Port: 143 Service: imap
Port: 443 Service: https
Port: 465 Service: smtps
Port: 587 Service: submission
Port: 993 Service: imaps
Port: 995 Service: pop3s
Port: 3306 Service: mysql (edited)


(292 kB) ▾



← → ↻ nav.no/.well-known/security.txt

Contact: soc@nav.no
Preferred-Languages: no, en
Canonical: <https://www.nav.no/.well-known/security.txt>
Disclosure: Full

SIKKERHET
Amedia utsatt for alvorlig dataangrep
Natt til tirsdag ble flere av Amedias sentrale datasystemer satt ut av drift. Ingen papiraviser blir publisert onsdag.



Framtidsrettet endring i Telenor

- 2 år siden
- Interne team
- Angripe oss selv
- Direkte samarbeid med konsulenter
- Vi jobber i **red team**
- Appsec = **purple team**
- TCERT + TSOC = **blue team**

RED TEAM



OFFENSIVT ANGREPSTEAM

Oppgaver inkluderer:

- Etisk hacking
- Simulere angriper
- Fysiske angrep
- Pentesting
- Black Box Testing
- Sosial manipulering
- Web scanning

PURPLE TEAM



DATAINNSAMLING OG IMPLEMENTERINGSTEAM

Oppgaver inkluderer:

- Dataanalyse
- Samarbeidssikkerhet
- Rød mot Blå
- Ferdighetstesting
- Systemforbedringer

BLUE TEAM



DEFENSIVT BESKYTTELSESTEAM

Oppgaver inkluderer:

- Infrastruktursikkerhet
- Skadekontroll
- Hendelseshåndtering
- Trusseljakt
- Digital etterforskning
- Sikkerhetsbevissthet





Sikkerhetstips



Sikkerhetsutfordring

Rekk opp en hånd hvis du...



Hvis du bruker tofaktor (2FA) på eposten din



Bruker samme passord flere steder



Lagrer passord i nettleseren din/i en ulåst fil/notat



Om du rakk opp hånda på en av disse har du blitt «hacket»



Sikkerhetstips



Bruk 2FA (To faktor autentisering) der du kan



Ikke lagre passord i nettleseren din (Password manager)



Ikke gjenbruk passord



Sjekk eposten din på haveibeenpwned.com og telenor.no/tryggepost



Sjekk maskinen din med antivirus hver uke



Ta backups!

Sjekk om din e-postadresse er på aweie

Skriv inn e-postadressen i feltet under (vi lagrer ikke adressen)

✉ jens@online.no



Søk

Uff da! Vi har funnet 23 sikkerhetsbrudd på denne e-postadressen. Dette betyr at uvedkommende kan utnytte din personlige informasjon. Men pust rolig, vi hjelper deg.

Dette må du gjøre nå:

- **Endre passord** på alle kontoene/tjenestene som e-postadressen er knyttet til.
- Vi anbefaler at du bytter passord på dine tjenester med jevne mellomrom, og at du **ikke bruker samme passord flere steder**. Les hvordan du kan lage sterke passord [her](#).

!;--have i been pwned?

Check if your email or phone is in a data breach

jens@online.no

pwned?

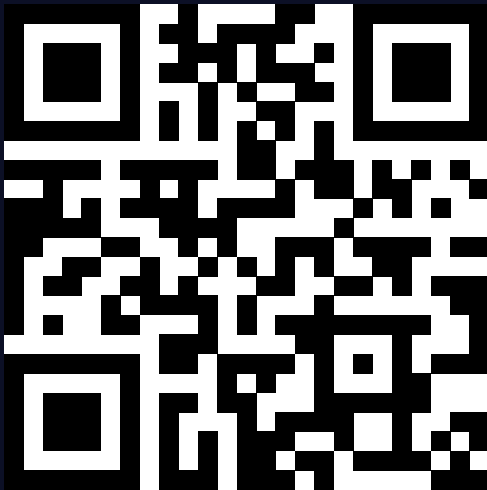
Oh no — pwned!

Pwned in 16 data breaches and found 2 pastes (subscribe to search sensitive breaches)





Takk for meg!



in



[linkedin.com/in/-daniel-](https://www.linkedin.com/in/-daniel-)



[tiktok.com/@bobtheshoplifter](https://www.tiktok.com/@bobtheshoplifter)



20.no/discord

