METODERAPPORT DATA-SKUP 2018

Jakten på «Edderkoppen»

Journalister: **Henrik Lied**, **Trude Furuly** og **Truls Antonsen** (fotograf)
Utviklere: **Johannes Odland** og **Glen Imrie**

NRK Bjørnstjerne Bjørnsons plass 1, 0340 Oslo

1. Innledning

Maiken Skoie Brustad er egentlig ganske fornøyd med seg selv og livet. Hun er veltrent, hun har vært modell og har deltatt i Miss Norway. Og nå har hun akkurat fått ny jobb som personlig trener – i London.

23-åringen står og småprater med personalet i en av metropolens vintagebutikker da meldingen tikker inn. Meldingen som blir starten på et to år langt mareritt.

Maiken skulle flere år senere vise seg å være ett av «Edderkoppens» mange ofre. Fra hjemmet sitt brukte han datamaskinen til å trakassere og rundlure kvinner over hele landet i over seks år.

Under dekke av flere titalls falske identiteter, og med ganske elementære datakunnskaper, kom han i kontakt med intetanende kvinner.

Politiet klarte aldri å finne mannen, til tross for at flere politidistrikt hadde fått anmeldelser og tips om aktivitetene hans. NRK fant ham.

I denne rapporten redegjør vi for hvordan vi gjennom syv måneders møysommelig arbeid nøstet oss frem langs trådene i hans intrikate nett, før vi til slutt avslørte «Edderkoppen».

2. Slik startet det

I november 2017 skulle NRK Nyheter lage en sak om ulovlig spredning av nakenbilder. Dette var et voksende problem, som fikk mye oppmerksomhet i media etter #Metoo og Nora Mørk-sakene. Etter research og tips om mulige caser, dukket navnet Maiken Skoie Brustad opp. Det lå mange meget intime bilder av Maiken på nett, og journalist Trude Furuly tok kontakt med henne. I en telefonsamtale fortalte Maiken om hva som skjedde med henne etter at nakenbildene hadde havnet på nett. Historien var hjerteskjærende.

Da Maiken i 2016 oppdaget at hennes private bilder lå på nett, var hun desperat etter hjelp, og hun kontaktet den norske veiledningstjenesten Slettmeg.no. Få timer etterpå fikk Maiken en e-post som skulle bli skjebnesvanger.

E-posten var fra en mann som presenterte seg som «Oscar Persson» fra «Slettamig.se». Han opplyste at det var den svenske delen av det statlige foretaket «Slettmeg.no». Mannen fremsto som meget troverdig. Han hadde profesjonelt språk, og viste til lignende saker han hadde løst, og han oppga at han hadde dyktige samarbeidspartnere, blant annet en datakonsulent i USA. Alt dette var usant, men Maiken fikk umiddelbart tillit til «Oscar».

Det tok lang tid før Maiken oppdaget at hverken «Oscar Persson», eller firmaet han jobbet for eksisterte. I prosjektperioden brukte vi navnet «Oscar Persson», men i de publiserte sakene kalte vi ham også «Edderkoppen».

Samtalene mellom Maiken og «Oscar Persson» på e-post og andre steder, viste hvor kynisk han opererte. Under dekke av å ville hjelpe Maiken, ba han om informasjon som kunne gjøre situasjonen enda verre for henne.

I en e-post skrev «Oscar»: *«Hvem utenom dine sexpartnere har kjennskap til sexlivet ditt, og har du noen gang hatt sex på steder hvor andre kan ha sett / fanget dett opp, kan du i såfall bekrefte for meg hvor og når.»*

Han kom stadig med løfter om at han var nær å finne den som hadde delt bildene: *«Pust helt rolig Maiken. Jeg kan informere deg om at jeg allerede har begynt å identifisere mennesker som laster ned bilder [..].»*

Samtidig dro han gradvis ut mer og mer informasjon av Maiken: *«Er det noen, spesielt gutter du ikke kjenner / kjenner dårlige / via / via som har kontaktet deg på f.eks sosiale medier det siste året som du har avviset? Eller noen du kjenner, som har gitt deg uønsket oppmerksomhet/dårlige vibber? Vi utelukker nå effektivt identiteter vi har, opp mot identiteter du gir oss».*

Etter å ha lest gjennom korrespondansen hadde vi vanskeligheter med å tro at noen skulle bruke så mye tid og krefter på bare én person.

Kunne Maiken være bare ett av flere ofre?

Hvem var denne såkalte «Oscar Persson»?

Vi klarte ikke legge fra oss saken.

2.1 Hypoteser

Basert på «Oscars» språkbruk, profesjonalitet og måten manipulasjonen ble utført på i kommunikasjonen, utarbeidet vi flere hypoteser:

- Personen bak e-posten har drevet med nett-trakassering over lengre tid, og med flere ofre.

E-posten fra Slettamig.se kom bare timer etter at Maiken hadde kontaktet norske Slettmeg.no. Selv om dette kunne være en ren tilfeldighet, vurderte vi også følgende:

- Vedkommende har hatt tilgang til Maikens datamaskin eller e-posten til Slettmeg.no
- Dersom dette stemte, kunne det også bety at «Oscar» hadde hacket Maiken eller faktisk selv vært med på å spre bildene hennes – før han tilbød seg å hjelpe med å fjerne dem.

3. Derfor var saken viktig

Fri informasjon er internetts gyldne fane. Et sted hvor kunnskap demokratiseres, hvor alle har lik tilgang til informasjon og lik mulighet til å bli hørt og sett. Men frihetsfesten har sine kjellerparties – informasjon blir misbrukt, avsendere forfalskes, bilder stjeles, manipuleres og publiseres for all verden. Menneskeliv blir lagt i ruiner. For noen blir følgene fatale. Norsk politi gikk i mars ut med historien om den unge mannen som begikk selvmord etter å ha blitt seksuelt utpresset av nettsvindlere.

Vi hadde en oppfatning om at det var for lett å komme unna med ulovlig spredning av bilder, trusler og trakassering på nett. Inntrykket vårt var at politiet ikke alltid prioriterte disse sakene, og at den psykiske belastningen og de personlige konsekvensene ofte var enorme. Ikke alle som ble ofre for slikt orket å snakke høyt om det eller stå frem i media.

Maiken klarte i perioder ikke å gå på jobb, og begynte hos psykolog da hun forstod at hun hadde blitt lurt av «Oscar». Han fortsatte å ta kontakt gjennom andre kanaler på nett. Hun anmeldte hendelsen til politiet. På grunn av mangel på bevis, ble saken henlagt etter kort tid.

Da henleggelsen kom, følte Maiken seg alene og hjelpeløs. To år senere satt hun fortsatt uten svar. Det var flere spor å følge, og dersom noen ville gjøre et forsøk i å nøste i «Oscars» identitet, ville det bety mye for henne. Samtidig kunne en sak kanskje få betydning for enda flere – tenk om personen bak aliaset «Oscar Persson» lurte mange andre?
Der og da bestemte vi oss for at dette ikke bare skulle bli en historie om ofre – vi ville finne gjerningsmannen. Det skulle bli mye, mye mer krevende enn vi trodde.

4. Slik organiserte vi oss

Prosjektet har vært et utpreget samarbeidsprosjekt mellom flere avdelinger i NRK. Helt i begynnelsen jobbet Trude Furuly og fotograf Truls Antonsen i NRK Nyheter med saken, men raskt ble NRKBeta-journalist Henrik Lied, og utviklerne Johannes Odland og Glen Imrie i Digital Historieutvikling en del av teamet.

Etter grønt lys fra sjefer, booket vi et prosjektrom hvor vi kunne arbeide skjermet over lengre tid. På prosjektrommet hadde vi storskjerm og plass til å henge opp oversikt på tavle og vegger, som hjalp oss å holde system i arbeidet.

Fra januar 2018 ble de fleste i teamet i perioder tatt ut av vanlige arbeidsoppgaver for å jobbe mer eller mindre fulltid med prosjektet. I tiden før publisering ble illustratør Marco Vaglieri, fotograf Patrick da Silva Sæther, skrivecoach Mads Nyborg Støstad og nyhetsjournalist Camilla Wernersen koblet på.

5. Slik gjorde vi det

5.1 Fase 1 – Innledende undersøkelser

«Oscar» kommuniserte med Maiken på e-post og Facebook i en lang periode, med løfter om å hjelpe med å fjerne nakenbildene fra nett. Etterhvert flyttet han samtalen over på krypterte tjenester for å holde samtalen hemmelig. De kunne chatte sammen til langt på natt, og han dro gradvis mer og mer informasjon ut av Maiken. Samtidig fikk han henne til å mistenke venner og familie. Han kom stadig med løfter og påstander om at han nærmet seg å finne den som stod bak bildespredningen, og jobbet med å lage en politianmeldelse Maiken kunne bruke. Han sa også at han hadde funnet en video av henne hvor hun ble voldtatt, mens hun var veldig beruset. Hun har i ettertid blitt helt sikker på at dette ikke har skjedd.

Etter flere ukers kontakt avtalte de å møtes på Torp flyplass for å forberede rettssak mot den som hadde stått bak bildespredningen. Først da Maiken og moren møtte opp på Torp flyplass, og «Oscar» ikke dukket opp, forsto hun at «hennes gode hjelper» hadde lurt henne.

Selv om Maiken sluttet å skrive med «Oscar» fortsatte hun å få trakasserende meldinger på e-post og i sosiale medier. Hun fikk stadig nye e-poster med truende innhold fra en rekke anonyme avsendere. Mye tydet på at «Oscar» stod bak meldingene.

Maiken hadde tatt vare på mye av kommunikasjonen med «Oscar» i form av e-post og skjermkopier av facebook-samtaler. Dette, sammen med politianmeldelsen, ga oss et godt innblikk i saken. Men vi trengte en systematisert oversikt for å finne ut hvordan vi skulle nøste videre.

Vi plottet derfor alle hendelser inn i en tidslinje, med dato og klokkeslett. I lange intervjuer med Maiken spurte vi om detaljer som manglet og spørsmål som var ubesvart. Vi snakket også med Maikens mor på telefon for å få flere detaljer på plass.

Oversikten viste oss et tydelig hendelsesforløp. Vi fant det mistenkelig at «Oscar» kontaktet Maiken bare timer etter at hun hadde kontaktet Slettmeg.no på e-post. *Hadde «Oscar» tilgang til e-posten hennes, hadde han tilgang til e-posten til Slettmeg.no, eller var det bare et tilfeldig sammentreff?*

Den store mengden e-post og kommunikasjon var et godt utgangspunkt for videre graving.

Sporene på Maikens PC

Dersom «Oscar» hadde hatt tilgang til Maikens maskin eller e-postkonto, kunne han ha lagt igjen spor. Heldigvis hadde vi tilgang til stedet sporene kunne ligge: Maikens datamaskin. Datajournalist Henrik Lied gjennomsøkte maskinen og lette etter følgende:

1. Metadata i e-poster

I en e-post ligger det ofte mer informasjon enn det som er synlig for det blotte øyet. Dette kalles e-postens «header». I headeren kan det ligge informasjon som kan si noe om avsender, som for eksempel hvilken nettadresse e-posten er sendt fra. I headerene på e-poster fra «Oscar» fant vi en referanse til en norsk domeneleverandør. Det sannsynliggjorde at personen som stod bak domenet Slettamig.se hadde registrert det i Norge, noe som var oppmuntrende.

2. Elementer i e-poster som kunne inneholde informasjon

Korrespondansen mellom Maiken og «Oscar» ble finkjemmet for informasjon som kunne avsløre hvem som var avsenderen. Hvis «Oscar» hadde sendt bilder eller filer til Maiken, kunne de inneholde metadata som for eksempel IP-adresser eller geografiske koordinater i EXIF-dataene. Vi fant filer, men her var alt av personlig identifiserbar informasjon skrubbet bort.

3. Tegn på at brukerkontoene hennes hadde blitt eller var forsøkt kompromittert

Hadde noen av kontoene til Maiken (PC, e-post, Facebook-bruker o.l) blitt kompromittert, og var det derfor bildene av henne hadde lekket? Kunne også «Oscar» ha vært bilde-deleren?

Dersom noen utenforstående prøver å komme seg inn på brukerkontoer på nett, kan dette bli registrert som mislykkede innloggingsforsøk i loggen i brukerkontoen. En gjennomgang av loggen til Maikens e-postkonto viste flere mislykkede innloggingsforsøk, med IP-adresser sporet til Russland og land i Asia.

Vi sjekket de aktuelle IP-adressene opp mot servere i Tor-nettverket. Tor-nettverket brukes ofte av ulike aktører som er ute etter å skjule sine spor, og er flittig brukt av kriminelle. Ingen av IP-adressene stammet derfra, så det var en mulighet for at disse påloggingsforsøkene kun var automatiserte tjenester som forsøker å logge seg inn på kontoer som er kompromitterte.

For å sjekke om noen av Maikens andre brukerkontoer hadde blitt kompromittert, brukte vi nettstedet «Have I been pwned». Dette nettstedet har en oversikt over brukerkontoer som har blitt kompromittert i datalekkasjer. Ved å legge inn e-post kan man finne ut om brukere tilknyttet e-postadressen har blitt kompromittert. Brukerinformasjon tilhørende Maiken hadde blitt delt i minst fire datalekkasjer: To av disse inneholdt gamle passord, mens to inneholdt passord som var ekstra sikret. Men ingen av passordene var lenger i bruk.

Undersøkelsene på Maikens data ga ingen store resultater. Vi fant ikke noe grunnlag for å påvise at «Oscar» kontrollerte Maikens e-post eller at han sto bak selve bildedelingen, og la denne hypotesen til side. Brukerinformasjon tilhørende Maiken hadde tidligere blitt lekket, men vi antok at det ikke hadde stor betydning fordi passordene som var lekket ikke lenger var i bruk. Det eneste konkrete vi fikk ut av undersøkelsene var en indikasjon på at domenet slettamig.se hadde blitt registrert i Norge da det ble opprettet.

Tips 1: Nettstedet «Have I been pwned» (https://haveibeenpwned.com/) har oversikt over brukerkontoer som har blitt kompromittert i datalekkasjer. Nettstedet lar deg søke med en e-postadresse for å se om brukeren har blitt kompromittert.

Tips 2: Bilder inneholder ofte EXIF-metadata. Dette kan være informasjon om når bildet ble tatt, og hvilket kamera som ble brukt. Det kan også være geografiske koordinater. Denne metadataen kan hentes frem i mange bildeprogram, som f.eks. preview på mac.

Tips 3: I e-postheadere kan det ofte ligge identifiserende informasjon. Ofte finner man informasjon om hvilken e-postklient avsenderen har brukt for å sende meldingen, avsenders IP-adresse, og hvilke navne- og mailservere som meldingen har gått gjennom. Hvordan man sjekker e-postheadere avhenger av hvilken e-postklient man bruker. I Gmail-universet trykker man på pilen i øvre høyre hjørne av en e-post, og velger "Show original".

Slettmeg.no og Slettamig.se

Vi måtte komme til bunns i om det fantes koblinger mellom Slettmeg.no og Slettamig.se. Vi gjorde research på Slettamig.se og hvem som eide det. Med et nettsøk fant vi en artikkel fra 2016, hvor Norsk senter for informasjonssikring (NorSIS, som eier Slettmeg.no) advarte mot en falsk utgave av Slettmeg.no. Og så kom en setning som viste med all tydelighet at det var gode grunner for å gjøre jakten på «Oscar Persson» til et journalistisk prosjekt: Flere jenter, skrev NorSIS, hadde blitt kontaktet av en som kalte seg «Oscar Persson». NorSIS opplyste også at de hadde varslet politiet om saken. Hendelsen hadde altså blitt omtalt av NorSIS tidligere, men hadde utover dette fått lite medieoppmerksomhet.

På bakgrunn av artikkelen kontaktet vi Slettmeg.no for å høre om vi kunne få mer informasjon. De begrenset seg i stor grad til å bekrefte det som allerede var omtalt i 2016. Vi fikk ellers ingen andre treff på Slettamig.se i søk på nett. Det var umulig å finne noe informasjon på nettet som tilsa at Slettamig.se på noe tidspunkt hadde vært et reelt selskap.

Allerede nå fikk vi en bekreftelse på hypotesen vår om at det fantes flere ofre.

De første viktige sporene

Undersøkelsene av Maikens datamaskin førte ikke langt nok, og vi måtte nå ta utgangspunkt i det viktigste digitale sporet vi hadde: e-postadressen oscar@slettamig.se. E-posten tilhørte et svensk domene (sluttet på .se), og navnet var basert på det som tilsynelatende var et falskt selskap. Vi antok at personen som sendte e-poster fra domenet Slettamig.se var den samme personen som hadde opprettet domenet, og arbeidet ut i fra dette.

Dersom vi kunne finne ut hvem som hadde opprettet «Slettamig.se» kunne vi kanskje også avsløre «Oscar».

Når et domene opprettes, registreres dato for opprettelse sammen med kontaktinformasjon til eier og hvilken registrar som er ansvarlig. Denne informasjonen kan man finne med et WHOIS-søk. Et søk på «Slettamig.se» ga oss begrenset med informasjon fordi

kontaktinformasjonen var anonymisert.

Noe av informasjonen var likevel synlig. Domenet var opprettet i 2015, og var koblet til en norsk navneserver. Et søk i Wayback Machine viste at det neppe hadde vært noen hjemmeside knyttet til domenet. Hadde domenet tilhørt en reell organisasjon, ville det mest sannsynlig hatt en hjemmeside i løpet av de siste tre årene, konkluderte vi med. Vi mistenkte at domenet var opprettet av «Oscar», for å fremstå som en troverdig representant for Slettmeg.no.

Tips 4: WHOIS lar deg søke opp registreringsinformasjon til et domene. Her kan du finne når domenet ble opprettet og når det ble oppdatert. Det kan også være mulig å lese hvem som er eier av domenet og hvilken registrar som er benyttet. DomainTools har en WHOIS-tjeneste her: http://whois.domaintools.com/

Tips 5: Wayback Machine hos Internet Archive er et historisk arkiv av hjemmesider. Tjenesten gjennomsøker jevnlig nettet og lagrer kopier av nettsider som de så legger ut på et gitt tidspunkt. Archive.is er en lignende tjeneste som også har kopier av mange nettsider, og som man enkelt kan be om å arkivere en eksisterende nettside.

Reverserte søk basert på falsk informasjon

Fordi mye informasjon var anonymisert i Whois-resultatet, kontaktet vi Internetstiftelsen i Sverige (IIS) som driver toppnivådomenet «.se», og registeret for alle .se-domener. IIS har informasjon som navn, adresser og telefonnummer til eiere av domener som slutter på «.se». IIS meldte tilbake at det skulle være mulig for oss å få mer informasjon fordi domenet var privateid. Men de leverte ikke ut slik informasjon uten videre, og vi måtte derfor sende en skriftlig og begrunnet søknad, som skulle vurderes av jurist.

Vi ventet spent på svar. Et par uker senere var søknaden innvilget og vi fikk kontaktinformasjonen til den som hadde registrert domenet Slettamig.se. Vi følte at vi var på sporet av noe. Og vi hadde navnet på en mann.

Idet vi begynte å gå informasjonen nærmere etter i sømmene, viste det seg at den var delvis eller helt falsk. Navnet vi fikk tilhørte en person som etter alt å dømme ikke hadde noe med saken å gjøre. Mobilnummeret var ikke lenger i bruk, og e-postadressen inneholdt ikke navn eller andre ledetråder.

Det ble tydelig at den vi lette etter gjorde aktive forsøk på å skjule sporene sine. Det trigget oss til å fortsette. Vi begynte å søke med kontaktinformasjonen i flere offentlige register på nett, som Domaintools, DomainBigData og SecurityTrails som har oversikt over domener og eiere.

Den falske kontaktinformasjonen ble selve nøkkelen til å komme videre. Flere domener som inneholdt anerkjente merkevarer og navn, hadde blitt registrert på den samme falske kontaktinformasjonen. Nå hadde vi plutselig mer informasjon å gå etter i videre graving.

Tips 6: Falsk informasjon kan også være viktig informasjon. Folk kan etter hvert miste kreativiteten og begynne å gjenbruke den falske informasjonen. Dermed røper de at det kan være samme person som står bak aktivitet på forskjellige domener.

Tips 7: SecurityTrails lar deg søke opp aktive domener basert på kontaktinformasjon som telefonnummer og e-postadresse. Domaintools har historiske data, som betyr at du kan få oversikt over historikken til et domene, for eksempel når det ble opprettet eller slettet. Det er derimot uvisst hvordan fremtiden til WHOIS-systemet blir når GDPR går i full kraft.

Systematisering, første runde

Etter hvert hadde vi fått mange ledetråder. Vi hadde kommunikasjon mellom Maiken og «Oscar», navn, adresser, telefonnumre, e-poster og domener. Vi måtte sikre at vi klarte å holde oversikten.

Vi opprettet en tidslinje (regneark). Her registrerte vi når domener hadde blitt opprettet og slettet, når e-poster hadde blitt sendt, fra hvilke e-postadresser og når andre kontoer var aktive. Vi registrerte også nøye tidspunktene på døgnet «Oscar» kommuniserte med Maiken. Vi brukte et regneark for å lage denne oversikten, med tid langs den horisontale aksen, og identiteter som e-post og domene langs den vertikale aksen.

For å få oversikt over ledetrådene vi hadde, opprettet vi en egen oversikt. Vi noterte ned ledetråden, hvor vi hadde den fra og hvilke nye opplysninger den ga oss. Ledetrådene dannet en graf, hvor en ledetråd ledet til flere andre. Vi laget en digital oversikt over mengden ledetråder og ledd.

Vi måtte ta høyde for at noen av de nye ledetrådene ikke nødvendigvis hadde noe med «Oscar» å gjøre. Vi registrerte derfor også med hvor stor sikkerhet vi kunne knytte ledetråden direkte til «Oscar». Hver gang vi fant en ny ledetråd måtte vi nøye gå gjennom oversikten og vurdere hvor sikkert eller usikkert det var at hver ledetråd var knyttet til «Oscar». Vi ga hver ledetråd en sannsynlighetsgrad, og oppdaterte denne dersom nye opplysninger kom til fra andre kilder.

Denne måten å organisere materialet på, skulle etter hvert gi oss et viktig gjennombrudd. (Se side 14).

De interne oversiktene over materialet ga oss ikke bare orden i sysakene, men også et sett med domener og e-poster vi visste «Oscar» stod bak. Oversiktene viste at han hadde holdt på i flere år.

5.2 Fase 2 – Utvidet søk

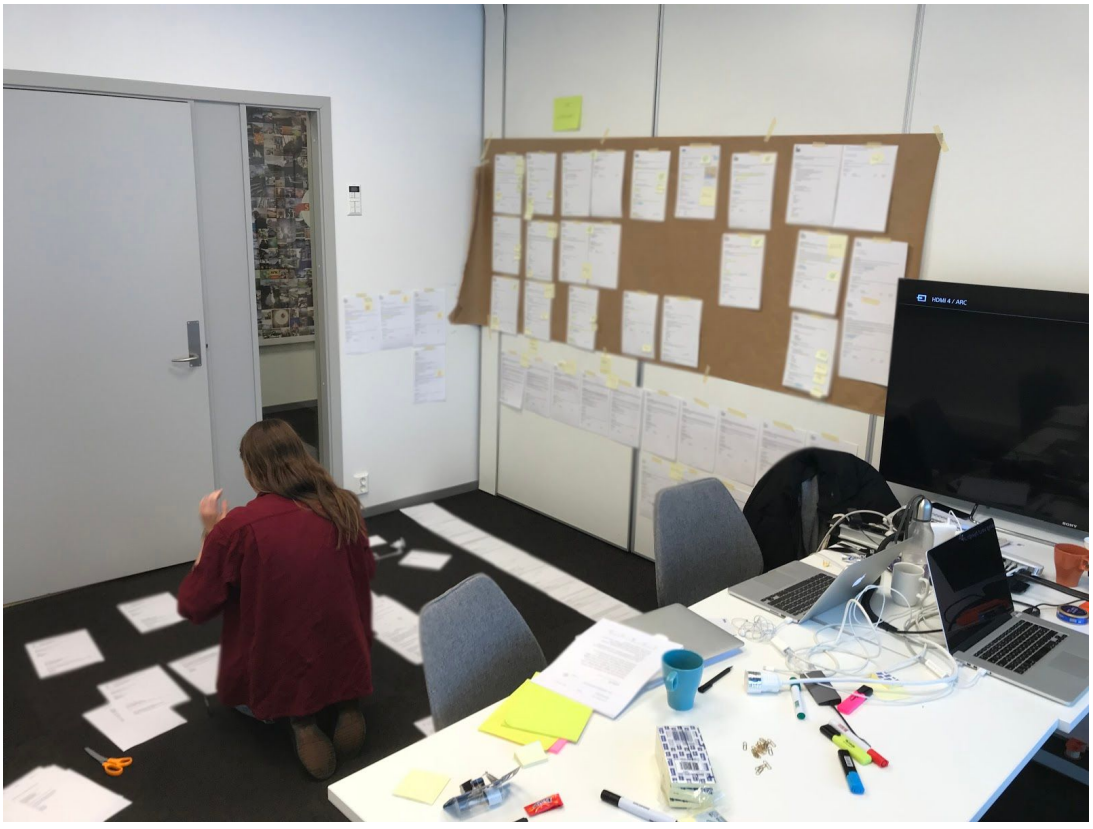
På dette tidspunktet var vi klar over at den falske kontaktinformasjonen ikke var nytteløs, men faktisk en gullgruve med informasjon. Vi gikk grundig gjennom all kontaktinformasjon vi var kjent med punkt for punkt. Kunne det hende kontaktinformasjonen hadde blitt brukt enda flere steder?

Vi puttet ulik kontaktinformasjon vi hadde samlet opp inn i begrensede nettsøk (se tips 8) - og ble sittende forbløffet å se på resultatene. Vi fikk vi flere treff - på gamle stillingsannonser. De fleste lå åpent tilgjengelig på Karrierestart.no, og det var egentlig ikke noe bemerkelsesverdig med annonsene ved første øyekast. Det endret seg da vi tok en nærmere titt.

Tips 8: Du kan begrense et nettsøk hos Google til å gjelde kun et nettsted. For å finne informasjon på dette nettstedet kan du legge inn «site:eksempel.no» i søket. For eksempel: «edderkoppen site:nrk.no»

Analyse av annonser

Vi samlet annonsene vi fant og hang de opp på prosjektrommet. Ved å legge de ved siden av hverandre kunne vi enklere finne likheter eller ulikheter mellom annonsene. Med gul tusj markerte vi ord, setninger, oppgitte adresser og e-poster i annonsene.



Teamet hadde tilhold på dette prosjektkontoret på Marienlyst. Foto: Glen Imrie

Vi la merke til at stillingsannonsene hadde et særegent språk og inneholdt enkelte litt gammelmodige norske ord. Med inspirasjon fra tv-serien «The Unabomber» benyttet vi delsetninger og ord fra stillingsannonsene vi hadde funnet, til å søke opp enda flere. Vi fant ut at stillingsteksten noen ganger hadde blitt gjenbrukt med kun små eller uten endringer i andre annonser. Det tydet på at samme person sto bak.

Vi fant også flere andre likheter mellom annonsene. Det ble ofte brukt vilkårlige postadresser og de inneholdt sjelden telefonnummer, noe som var litt rart. En viktig fellesnevner vi fant var også at søknad utelukkende skulle sendes på e-post.

Hvis «Oscar» stod bak disse stillingsannonsene, var det en metode han brukte for å komme i kontakt med mulige ofre?

Stillingsannonsene hadde også en slags rød tråd. Stillingene som var utlyst var stort sett innenfor serviceyrker som bartender, reiseleder, personlig assistent og vert/vertinne til eventer. Det var sjelden krav til kvalifikasjoner, og opplæring kunne gis av arbeidsgiver.

Mange av annonsene var åpenbart falske. For eksempel søkte et lite firma med én ansatt etter 15 nye deltidsansatte. En rask telefon til firmaeier bekreftet at annonsen var en bløff. Og den oppgitte e-postadressen som søknader skulle sendes til gikk ikke til firmaet.

Vi hadde tidligere lagt merke til at «Oscar» ofte benyttet e-postadresser fra en utenlandsk e-postleverandør. Et bredt søk på annonser knyttet til denne leverandøren gjorde at vi fant enda flere annonser med lignende innhold.

I denne fasen søkte vi bredt etter jobbannonser. Derfor måtte vi ta høyde for at mange av annonsene vi fant ikke hadde noe som helst med «Oscar» å gjøre. Annonsene måtte sees i sammenheng med de andre domenene og e-postene vi visste han kontrollerte.

Dermed kunne vi, etter å ha silt ut mange annonser, være sikre på at et titalls av annonsene vi hadde funnet, var ført i pennen av «Oscar».

Innsyns-nei fra NAV

Noen av stillingene vi fant hos Karrierestart var hentet fra stillingsdatabasen til NAV. *Kunne det ligge mer informasjon i annonsene? Og kunne NAV ha andre annonser vi ikke hadde klart å finne?*

Vi ba om innsyn i alle NAVs jobbannonser fra 2009 frem til 2018, i håp om at det kunne gi oss noe mer. Det ble avslag. NAV svarte at jobben var for omfattende til at de kunne avsette ressurser. De foreslo en mulig løsning som ikke gjenspeilte vår forespørsel, og heller ikke i ivaretok våre behov.

Vi ville ikke gi oss, og i en ny e-post til NAV viste vi til Offentleglova §9: «Alle kan krevje innsyn i ei samanstilling av opplysningar som er elektronisk lagra i databasane til organet dersom samanstillinga kan gjerast med enkle framgangsmåtar.»

Vi påpekte at en eksport fra et moderne databasesystem ikke er en komplisert prosess. Vi viste også til at vi hadde forhørt oss med flere utviklere med kompetanse på de ulike teknologiene som var i bruk hos NAV. De kunne bekrefte at det vi ba om ikke var en omfattende jobb.

Vi påpekte også at utviklere i en offentlig NAV-video, som lå ute på nett, forteller om datasystemene de bruker i den aktuelle portalen. Vi tilbød oss også å ta i mot dataene i det formatet som var minst ressurskrevende for NAV.
Vi fikk innsyn.

Det fremgikk imidlertid av materialet vi fikk, at databasen var ufullstendig. Dermed måtte vi rette enda en henvendelse til NAV, og til slutt fikk vi hele materialet.

For lettere å kunne søke gjennom annonsene lastet vi dem inn i søkemotoren Solr. Søkemotoren gjør det mulig å søke i dokumenter på samme måte som en søker gjennom nettet med Google.

Tips 9: Solr kan også gi treff selv om ordet du søker etter ikke har blitt skrevet korrekt. Derfor er Solr et bra verktøy å bruke hvis man skal søke gjennom store mengder dokumenter som for eksempel jobbannonser, hvor det kan finnes feilstavinger.

Gjennom innsynet fikk vi også en ny og viktig opplysning. Vi så at flere av «Oscars» falske stillingsannonser var registrert via NAVs egen stillingsportal. Dette ble beklaget av NAV, i en av NRKs oppfølgingssaker, og NAV bedyret også at det jobbes med å bedre sikkerheten i systemet.

Vi trodde den vi var på utkikk etter fortsatt var aktiv, og ville derfor ikke gå glipp av nye annonser som kunne bli lagt ut. For å sikre at vi skulle få med oss dette, satte vi opp Google Alerts på kontaktinformasjonen vi hadde. Da ville vi bli varslet om nye annonser med samme kontaktinformasjon.

Selv om stillingsannonsene ga oss store mengder med ny informasjon, som dannet et bedre bilde over hvordan «Oscar» opererte, ledet ikke sporene oss til en fysisk person.

Tips 10: Med Google Alerts kan du bli varslet automatisk når ny informasjon blir tilgjengelig på nett. Får det angitte søket ditt et nytt treff, vil du bli varslet på e-post.

Kartlegging av kilder

Vi måtte gå bredere ut i jakten på nye ledetråder, og det fantes flere som kunne ha informasjon vi trengte. Vi lagde en liste over mulige kilder. Lista var lang:

- Eiere av kontaktinformasjon som var oppgitt å ha registrert ulike falske domener
- E-postleverandører og teleoperatører i inn- og utland
- Selskaper og privatpersoner som var blitt misbrukt i jobbannonser og e-poster
- Annonseportaler som NAV, Finn.no og Karrierestart
- Politiet

Av hensyn til kildevern er vi i dette kapittelet nødt til å være mindre konkrete i omtalen av kildematerialet.

Mange av kildene vi kontaktet ønsket ikke å bidra eller hadde ingen relevant informasjon. Etter hvert som vi kontaktet flere kilder fikk vi mer informasjon og nye opplysninger. Til slutt kom vi i kontakt med mange ofre.

Mye stod på spill for ofrene. Flere ønsket å bidra, men fryktet konsekvensene. De hadde tidligere blitt lurt med falske identiteter. Kunne de stole på at vi var de vi utga oss for å være? Det viste seg at flere av ofrene var vanskeligstilte småbarnsforeldre som hadde blitt lurt av falske annonser som «Oscar» hadde laget. I disse annonsene utga han seg for å være firmaer eller privatpersoner som ville gi penger til familier som ikke hadde råd til ferie. Noen hadde delt mye personlig informasjon med «Oscar» i tro om at han var en god hjelper. Etter at de fant ut at de hadde blitt lurt, fryktet de at informasjonen skulle bli brukt mot dem.

Derfor ville flere av disse personene møte oss fysisk før de ville fortelle sin historie. De ville heller ikke at det skulle bli kjent at de hadde snakket med oss. Vi jobbet mye med å bygge tillit, ved å møte kildene personlig, gi mulighet for å kommunisere gjennom krypterte kanaler (som Signal, en app som muliggjør kryptert kommunikasjon), og ved å være åpne om våre hensikter og hvorfor vi ville snakke med dem.

I denne fasen kom vi endelig i kontakt med en person som hadde snakket med «Oscar» på telefon. Flere kilder ga oss opplysninger om at personen de hadde vært i kontakt med var en mann, og ga en antagelse på hvor i landet han kom fra.

Etter en langvarig prosess, satt vi på en stor mengde kommunikasjon som involverte «Oscar». I dette materialet, som vi ikke kan referere detaljert fra, framstår Oscar som manipulerende, og en person som også benyttet seg av trakassering og trusler.

Fremgangsmåten var slående lik modusen i Maikens samtaler med «Oscar». I denne fasen av arbeidet vårt, bekreftet ofre våre antagelser om at «Oscar» aktivt hadde brukt annonser for å komme i kontakt med mulige ofre. Et overveldende flertall av kildene vi snakket med var kvinner som hadde blitt lurt eller forsøkt lurt på ulike måter.

Deler av materialet vi nå satt på, inneholdt også dokumenter og bilder fra «Oscar». Alt dette ble sjekket for metadata på samme måte som tidligere, med stort håp om at det kunne avsløre noe mer. Men alt vi gjennomsøkte var fullstendig strippet for informasjon.

Det er imidlertid vanskelig å bløffe på heltid: Vi fant ut at «Oscar» noen ganger hadde blandet sammen egne e-postkontoer. En e-post-samtale kunne starte på en konto, og fortsette på en annen. Noen ganger ble dette trolig gjort for at han skulle fremstå som flere personer, andre ganger så det ut til å være en glipp. Dette hjalp oss å knytte e-postene hans sammen. Vi kunne se at emnelinje og samtaleinnhold i e-postene var identiske da de plutselig fortsatte med en annen e-postadresse.

Hos enkelte e-postleverandører er det mulig å bytte ut avsender av en e-post. Man benytter da en «sender address». For mottakeren ser det ut som om e-posten kommer fra en annen adresse en den du faktisk sender i fra.

Fordi samtalene plutselig fortsatte fra en annen e-postadresse kunne det virke som om «Oscar» hadde brukt en «sender address» for å skjule adressen han egentlig sendte fra, men glemt å bytte ut avsenderen senere i samtalen.

Men viktigst for oss; vi kjente igjen e-postadressen som dukket opp. Vi hadde tidlig i prosjektet kommet over den i forbindelse med en falsk jobbannonse fra 2012. Men vi fant da ingen tydelig tilknytning til Oscar, og derfor ble e-postadressen lagt inn i regnearket merket «Lav sannsynlighetsgrad».

Nå visste vi at Oscar hadde brukt den. Dermed ble den tidlige registreringen viktig for oss: Den viste at han hadde holdt på med falske annonser allerede for seks år siden.

Dette funnet var en fin pay off for at vi hadde tatt vare på og lagt inn alle opplysninger i regnearket.

Glippen hans ga oss også et håp:

Kunne «Oscar» noen gang ha gjort en feil som ville være nok til å identifisere ham?

Partsinnsyn

På dette tidspunktet oppdaget vi noe som satte oss i en spesiell situasjon: Kildeinformasjon viste at også NRK hadde blitt misbrukt av «Oscar». Høsten 2016 var det flere medieoppslag om unge jenter som på e-post hadde blitt forsøkt lokket til en falsk Skam-audition. NRK så alvorlig på saken, og hadde anmeldt misbruket til politiet. Vi visste nå at «Oscar» sto bak bedraget.

Det at bedriften NRK AS var en part i saken reiste noen problemstillinger. Ble vår rolle på noen måte endret av dette, og hvordan kunne det påvirke det journalistiske arbeidet med saken? Etter en runde med redaktører og juridisk avdeling i NRK, kom vi frem til at vårt redaksjonelle arbeid ikke burde eller skulle endre seg som følge av en sak NRK administrativt hadde vært involvert i. Det redaksjonelle arbeidet startet helt uten kunnskap om at NRKs bedriftsnavn hadde blitt misbrukt, og når det nå kom opp, var det rett og naturlig å behandle NRKs administrasjon som en kilde til informasjon – på lik linje med andre kilder.

Politiet begynte å etterforske Skam-saken, men den ble senere henlagt. Som part i saken hadde NRK partsinnsyn, og de i bedriften som var involvert i saken i 2016 hadde også annen nyttig informasjon vi nå tilegnet oss så langt det var mulig.

Ved å gå gjennom politiets saksdokumenter fikk vi bekreftet mange av opplysningene vi allerede hadde. Dokumentene viste også at vi hadde kartlagt mer enn politiet hadde gjort, før saken ble henlagt. Vi så en større sammenheng enn politiet hadde sett.

Systematisering, andre runde

Vi fortsatte å systematisere og vekte nye ledetråder. Når var jobbannonsene utlyst? Når var domenene opprettet og hvor lenge hadde de vært aktive? Når på døgnet hadde kommunikasjonen foregått? Hvilke nye navn, adresser, e-postadresser, og telefonnummer hadde vi funnet siden sist? Alt måtte inn i den digitale tidslinjen.

Oversikten viste en utvikling over tid, og at metodene ble mer utspekulerte. Gjennom tidslinja oppdaget vi et nytt mønster i «Oscars» modus operandi. Han startet en utbredt praksis med å opprette domener der han framsto som et firma. Med de nye domene virket han mer troverdig.

Feil mistenkt

Nå hadde vi en stor oversikt over e-poster og domener vi kunne knytte til «Oscar». Vi visste til og med hvor i landet han kom fra. Det eneste vi manglet var hans fysiske identitet.

På dette tidspunktet, og med et bredere overblikk over «Oscars» virksomhet, kunne vi gå til kildene igjen med ny informasjon. Flere kilder vi kom i kontakt med ledet oss nå mot en konkret person. Dette fremsto som et stort gjennombrudd i saken – hadde vi endelig klart å knytte et virkelig navn og en reell identitet til «Oscar»? Vi begynte å gjøre intensiv research på vedkommende, gjennom offentlige registre, sosiale medier og tidligere medieomtale.

Det var mye som passet, men vi kunne ikke overse at det var ting som skurret da vi begynte å sjekke ham opp mot vår egen tidslinje. Den aktuelle personen jobbet mye på kveldstid og natt. Dette sammenfalt svært dårlig med tidspunktene på døgnet vi i vår tidslinje hadde registrert at «Oscar» var aktiv. I tillegg stemte språkbruk i kildematerialet dårlig med nasjonaliteten til personen som var blinket ut. Personen måtte til slutt avskrives.

Siste forsøk

Vi hadde fulgt alle sporene vi kunne, og hadde mengder med informasjon, men vi hadde fortsatt ikke funnet ut hvem «Oscar» var. Arbeidet var tungt og trått. Vi begynte å tvile på om det var forsvarlig å bruke ressurser på videre graving. I hele prosessen hadde vi gjort det vi kunne for å unngå at den antatt meget datakyndige «Oscar», skulle merke at vi gikk ham og hans virksomhet etter i sømmene. Nå måtte vi justere taktikken.

Var det noe viktig vi hadde oversett eller noen metoder vi ikke kjente til? Vi leide inn en ekstern IT-konsulent som hadde høy kompetanse på digital sporing. Etter noen dagers arbeid konkluderte vedkommende med at det gjenstod få andre alternativer enn å prøve omstridte og potensielt ulovlige metoder for å finne «Oscar». Konklusjonen var en viktig bekreftelse å få, men det var likevel nedslående fordi vi ikke så flere muligheter for å komme videre i arbeidet. Det var selvsagt ikke aktuelt å bruke ulovlige metoder.

Etter konklusjonen fra konsulenten hadde vi en runde med redaktører om vi kunne sende en e-post med falsk avsender og skjult innhold til «Oscar», som kunne gjøre det mulig å avsløre identiteten hans. Det kunne for eksempel være en e-post med et bilde som lå plassert på

NRKs server. Idet mottakeren av e-posten åpnet den, ville bildet fra NRKs server bli hentet til vedkommendes maskin. Siden NRK kontrollerte denne serveren, ville det dermed vært mulig å logge informasjon om personen som hentet bildet.

Dette var åpenbart presseetisk utfordrende. Ifølge Vær varsom-plakatens punkt 3.10 skal journalister kun bruke falsk identitet i unntakstilfeller. Forutsetningen for dette må være «at dette er eneste mulighet til å avdekke forhold av vesentlig samfunnsmessig betydning». Det ble nei. Redaktørene konkluderte med at vi fortsatt hadde andre muligheter.

I stedet for å prøve å lure «Oscar» måtte vi heller åpent forsøke å opprette kontakt med ham. Vi kviet oss for å gjøre dette. Vi kjente fortsatt ikke identiteten hans, og fryktet at en slik fremgangsmåte ville få ham til å gå under jorda, slette kompromitterende materiale og fortsette å plage Maiken og andre kvinner fra nye identiteter.

Vi valgte en mellomløsning. Vi kjente til en e-postadresse «Oscar» nylig hadde brukt til å utgi seg for å være en som jobbet med å fjerne nakenbilder på nettet. En i teamet sendte en e-post og presenterte seg som journalist i NRK. Han skrev at han jobbet med den samme problematikken og gjerne ville møtes. E-posten var utformet slik at «Oscar» ikke skulle skjønne at vi visste mer.

Vi krysset fingrene. Raskt kom en e-post i retur: E-posten kunne ikke leveres til mottakeren fordi den ikke lenger eksisterte. Vi hadde ingen andre e-postadresser å ta kontakt med «Oscar» på, uten å blåse at vi var på sporet av ham. Nå gjensto bare én mulighet.

5.3 Fase 3 – Første publisering

Vi måtte publisere saken med nok informasjon slik at lesere gjennom tips kunne føre oss til hans ekte identitet. Publiseringen måtte planlegges nøye for å oppnå det vi ønsket. I artiklene ga vi ham kallenavnet «Edderkoppen».

Publisering som metode

Vi var et team med journalister, digitale utviklere, illustratører og designere som kjente saken godt og kunne jobbe effektivt med å lage hovedhistorien og oppfølgingssaker.

Saken skulle ut i mange flater: På nett, på TV, i radio og i sosiale medier. Det var viktig å nå bredt ut for at aktuelle tipsere skulle få med seg saken. Vi opprettet en egen tipstelefon som gikk direkte til oss, og la inn tipsboks i sakene som viste hvilke kanaler vi var tilgjengelige på.

22. april publiserte vi saken om «Edderkoppen», sammen med en kommentar som forklarte hvordan «Edderkoppen» i så mange år hadde klart å holde seg under radaren.

Vi fikk umiddelbart stor respons.

Nøkkeltipset

De første timene etter publisering kom det inn mange telefoner og henvendelser. Allerede samme dag kom tipset som senere skulle avsløre identiteten til «Edderkoppen».

Det tok tid å sjekke og følge opp tipsene som kom, og gjennomføre en systematisk kontroll av opplysninger mot informasjon vi allerede hadde registrert i tidslinjen vår.

En tipser fortalte at vedkommende for flere år siden hadde vært i kontakt med personen som måtte være «Oscar». Opplysninger fra denne kilden samsvarte med flere av de sentrale opplysningene vi allerede hadde. Tipseren oppga blant annet en e-postadresse vi kunne kryssjekke med informasjon i tidslinja.

Og aller viktigst: I deres kontakt begikk «Oscar» en feil – han hadde sendt fra seg metadata hvor hans ekte navn lå begravd.

Personresearch

Vi hadde nå endelig et navn og sterke indisier på at dette var rett person. Vi måtte fortsatt ta alle mulige forbehold i det videre arbeidet.

Med informasjon fra Folkeregisteret, skattelister, diverse nettsøk og kontoer i sosiale medier fikk vi dannet oss et bilde av personen. Vi hadde dokumentert at «Oscar» opptrådte hensynsløst og målrettet, og tenkte at han meget vel kunne være straffedømt. Vi sjekket domsregistre i nærheten av der han bodde. Det ble blink.

En dom fra flere år tilbake viste at mannen hadde begått lignende handlinger tidligere, og konkrete detaljer som adresser i dommen, sammenfalt med opplysninger vi hadde i vår oversikt. Dommen beskrev manipulative tendenser som minnet sterkt om de vi hadde sett i korrespondansen vi hadde lest.

I denne dommen kom det også frem opplysninger som gjorde at vi valgte å ikke identifisere mannen i våre saker.

Vi var nå sikre på at vi hadde funnet «Oscar».

5.4 Fase 4 – Konfrontasjon

Vi hadde mannen, og visste hvor han bodde. Vi slo av forskjellige grunner fra oss å oppsøke ham på hjemmeadressen.

Vi vurderte at den beste metoden var å ta kontakt med mannen på telefon og gjøre en avtale. Men nummeret var vanskelig å finne. Det var et stort paradoks. Med den store mengden kontaktinformasjon vi hadde samlet på ham det siste halvåret, skulle man tro det var en enkel sak å komme i kontakt med ham.

Vi fikk tak i nummeret til slutt. Da vi fikk kontakt med mannen, valgte han etter kort tid å legge kortene på bordet. Han gikk også med på å møte oss.

31. mai publiserte NRK avsløringen i alle flater, først på NRK.no med tittelen «Derfor manipulerte han norske kvinner på nett».

«Oscar», som tidligere er straffedømt, valgte å legge kortene på bordet da han møtte NRKs team. Han bekreftet at han i flere år har plaget kvinner på nett. Han bedyret overfor NRK at han ikke hadde noe med lekkasjen av Maikens bilder å gjøre. Foto: Truls Antonsen

6. Konsekvenser

- Etter to år i uvisshet kunne 25 år gamle Maiken Skoie Brustad og familien endelig gå videre. Maiken fikk også en personlig unnskyldning fra mannen som hadde gjort livet hennes til et mareritt. Hun har ikke blitt trakassert av ham igjen.

- NRK avdekket at det var en sammenheng mellom flere henlagte saker hos politiet. Artikkelserien belyste hvordan saker med ofre i forskjellige politidistrikt ikke ble sett i sammenheng.

- Norsk Senter for informasjonssikring har etter NRKs saker anmeldt misbruket til politiet, som etterforsker forholdet.

- Politiet undersøker også om Edderkoppen kan knyttes til andre saker.

7. Etikk

Anonymisering av «Oscar»

Vi identifiserte ikke «Oscar» i våre saker. Det lå en rekke vurderinger bak denne beslutningen. En totalvurdering av hans livssituasjon gjorde at vi ikke fant det riktig å identifisere ham. Av samme årsak kan vi ikke gå inn på innholdet i vurderingene.

Kildevern og forholdet til politiet

Politi og media kan ofte ha sammenfallende interesser, men har ulike roller og oppgaver i samfunnet. Som journalister kunne vi ikke overlevere upublisert materiale til politiet, til tross for at det kunne ha samfunnsmessige gevinster og bidra til å oppklare en politisak. Utad og til ofre var dette til tider krevende å formidle, kanskje særlig fordi vi ikke navnga «Oscar».

8. Nyttige erfaringer

Finne eier av et kontonummer: På et tidspunkt i prosjektet hadde vi et kontonummer vi var nokså sikre på kunne lede oss direkte til «Oscar». Dette er ikke nevnt tidligere i rapporten, fordi det viste seg å være et blindspor. Banker er underlagt svært strenge krav til personvern og kan ikke uten videre utlevere navnet på hvem som eier en konto til utenforstående. Men hos enkelte banker vil navnet på den som eier en konto likevel dukke opp i en kontoutskrift dersom man overfører penger til kontonummeret. Dette testet vi reportere oss i mellom ved å overføre små summer til hverandre. I enkelte banker dukket navnet på mottaker opp i transaksjonsoversikten etter at overføringen var bokført.

Finn navnet i Vipps: Noen ganger kunne vi ha telefonnumre, uten å vite hvilke personer de tilhørte. Nettsøk på numrene ga ingen treff eller viste at kundene var reservert mot nummeropplysning. I Vipps-appen var det i noen tilfeller likevel mulig å få opp navnet til personene ved å legge inn mobilnummeret i app-en.

Systematisering som metode: Systematiske oversikter er ikke bare viktig for å holde orden på materialet. Det kan også være en metode i gravingen. Det at både strukturerte data (som database-uttrekk) og ustrukturerte data som dokumenter, enkeltannonser, e-poster, navn og notater fra intervjuer var samlet i store oversikter var avgjørende for at vi klarte å trekke trådene sammen til slutt.

Digital tidslinje: Å lage en tidslinje hvor vi la inn når aktiviteten fant sted (år, måned, dag, klokkeslett) gjorde også at vi etter hvert som vi fikk flere datapunkter inn i systemet, kunne se akkurat hvilke ukedager og når på døgnet den vi lette etter var aktiv. Det var verdifull informasjon når vi senere fikk utpekt personer. Her bidro tidslinjen direkte til at vi oppdaget manglende samsvar mellom aktiviteten i vår tidslinje og arbeidssituasjonen til den utpekte.

Slik sjekket vi en person ut av saken.

Vedlegg

Oversikt over saker

I minst seks år har en ukjent person terrorisert norske kvinner på nett, 22.04.18:
https://www.nrk.no/edderkoppen-1.14011107

Maiken ble lurt av falsk versjon av Slettmeg.no - Søndagsrevyen 22.04.18:
https://tv.nrk.no/serie/dagsrevyen/NNFA03042218/22-04-2018#t=16m28s

Hvordan kan en person trakassere kvinner på nett i seks år uten å bli tatt? NRKBeta, 22.04.18:
https://nrkbeta.no/2018/04/22/hvordan-kan-en-person-trakassere-kvinner-pa-nett-i-seks-ar-uten-a-bli-tatt/

Finn, Nav, HBO Nordic, Unicef og Justin Bieber misbrukt av ukjent serietrakasserer, 23.04.18:
https://www.nrk.no/norge/store-aktorer-som-nav-og-finn-misbrukt-av-ukjent-serietrakasserer-1.14010972

Norske selskap misbrukt til å lure kvinner, radio 23.04.18:
https://radio.nrk.no/serie/dagsnytt/NPUB19011318/23-04-2018#t=51s
Lang og kort sak, pluss melding og snutt.

Nettrakasserere blir ikke tatt:
https://radio.nrk.no/serie/alltid-nyheter/MNAN02022818/23-04-2018#t=5m52.72s
https://radio.nrk.no/serie/her-og-naa-hovedsending/DMTN01008018/23-04-2018#t=26m36s
https://radio.nrk.no/serie/dagsnytt/NPUB09008018/23-04-2018#t=41s

Mener nettkriminelle bevisst utnytter systemsvakhet hos politiet, 23.04.18;
https://www.nrk.no/norge/mener-nettkriminelle-bevisst-utnytter-systemsvakhet-hos-politiet-1.14018587

Overlege: – Skambelagt å være offer for netthets, 24.04.18:
https://www.nrk.no/norge/overlege_-_-skambelagt-a-vaere-offer-for-netthets-1.14006100
https://radio.nrk.no/serie/dagsnytt/NPUB22011418/24-04-2018#t=1m39s

Maiken takker for støtten, 25.04.18:
https://www.nrk.no/norge/maiken-skoie-brustad-takker-all-for-stotten-1.14023321

Slik kan du unngå å bli et offer på nett, 27.04.18:
https://www.nrk.no/norge/slik-kan-du-unnga-a-bli-et-offer-pa-nett-1.13994683

Nettsending med panel som ble laget i kjølvannet av saken, 25.04.18:
https://www.nrk.no/norge/_-du-er-ikke-dum-fordi-du-sender-nakenbilder-til-kjaeresten-din-1.14022524

Mener politiet må snu rekrutteringa på hodet for å ta nettkriminelle, 26.04.18:
https://www.nrk.no/norge/mener-flere-it-folk-ma-inn-i-politiet-for-a-ta-nettkriminelle-1.14021291

Politidirektoratet direkte med i Dagsnytt, 26.04.18, for å svare på politiets datakompetanse. Oppspark med Politiforbundet, Politihøgskolen og Nito.
https://radio.nrk.no/serie/nyhetsmorgen/NPUB32008318/26-04-2018#t=1h3m0s

Dette er Edderkoppen, 31.05.18:
https://www.nrk.no/derfor-manipulerte-han-norske-kvinner-pa-nett-1.14063555

Her får Maiken beskjed om at Edderkoppen er funnet, 31.05.18:
https://www.nrk.no/norge/her-far-maiken-beskjed-om-at-_edderkoppen_-er-funnet-1.14063226

Dagsrevyen, intervju med Edderkoppen og Maiken, 31.05.18:
https://tv.nrk.no/serie/dagsrevyen/NNFA19053118/31-05-2018#t=1m25s

Bistandsadvokat mener Politiet har for få ressurser til å etterforske slike saker - Dagsrevyen 21, 31.05.18 (06:51):
https://tv.nrk.no/serie/dagsrevyen-21/NNFA21053118/31-05-2018

Politiet skal vurdere om Edderkoppen kan knyttes til andre saker - kan bli dømt etter ny straffelov, 01.06.18:
https://www.nrk.no/norge/politiet-skal-vurdere-om-_edderkoppen_-kan-knyttes-til-andre-saker-1.14065280

Netthetsere ønsker ofte oppmerksomhet, 01.06.18:
https://www.nrk.no/norge/forsker_-_-netthetsere-onsker-ofte-oppmerksomhet-1.14064357

Mener egen hjelpetelefon kan stanse netthetsere, 03.06.18:
https://www.nrk.no/norge/mener-egen-hjelpetelefon-kan-stanse-netthetsere-1.14066590