Dagbladet

Metoderapport
Data-SKUP 2019

SPAMMENS BAKMENN

Torgeir P. Krokfjord (Journalist), Tor Henning Ueland (Utvikler) og
Lars Eivind Bones (Fotograf)

INNHOLDSFORTEGNELSE

1. Innledning 3
Dette er saken 3
Bakgrunn 3
Slik startet det 3
2. Tekniske metoder 4
Systematisering og jakt på mønstre 4
Metode: Graving i nettsider 4
Metode: Crawler 5
Metode: Programmering 6
3. Jakten på bakmennene 7
Den franske milliardæren 7
Bakmennene avslører oss 8
Hjelperen «Jonas» 8
Metode: Whois-undersøkelser 9
Metode: Servergranskning 10
4. Gudfedrene 11
Muntlige kilder 11
Spor mot Tyskland 12
Metode: Graving i kildekode 12
Metode: Selskapssøk og sosiale medier 13
Metode: Bufrede Google-søk 13
Metal-referansen 14
Metode: E-postleting 15
Adelsmannen 15
Tysklandsturen 16
Konfrontasjonen 17
5. Presseetiske vurderinger 18
Forsøk på å stanse angrep 18
Trafikksammenligning 18
Skjult kamera 18
6. Konsekvenser 19
Vedlegg: LEnker til publiserte saker i prosjektet 20

1. INNLEDNING

Dette er saken

Dagbladet avslørte våren 2019 et omfattende dataangrep mot Dagbladet, VG, Aftenposten, BBC, Fylkesmannen, Statens Vegvesen og en rekke andre statlige og private aktører. Ved hjelp av metoder som programmering, innsamling og analyse av nettsider, selskapssøk i flere land, bruk av sosiale medier og kreativ jobbing i felt – avslørte vi hvem som sto bak og hvordan de opererer. For første gang ble bakmennene konfrontert.

Vi avdekket at det bak dataangrepet sto store, internasjonale markedsføringsaktører, som via såkalt «lead-generering» fikk samlet store mengder personopplysninger. Angrepet hadde til hensikt å tjene penger på salg av personopplysninger.

Saken fikk – som vi kommer tilbake til avslutningsvis – store konsekvenser i inn- og utland.

Men den startet som en liten tilfeldighet.

Bakgrunn

Etter at EU i mai 2018 innførte nye personvernregler – kjent som GDPR – er norske nettbrukere blitt vant til å trykke på samtykkemeldinger. Enten du skal lese en avis, handle i en nettbutikk eller se på nett-TV, må du trykke på en knapp som dukker opp på skjermen, der du aksepterer nettstedets personvernbetingelser.

Samtidig har det blusset opp en industri der personopplysninger på nett er en verdifull salgsvare og som tjener gode penger på å utnytte at forbrukerne er blitt vant til å trykke på samtykkemeldinger på PC-skjermen sin.

Stikkordet er «lead-generering» Det går i korte trekk ut på at publikum/nettbrukere lures til å gi fra seg e-postadresse, telefonnummer, personinfo eller kredittkortnummer, eksempelvis ved at de trykker på konkurranser på nettet.

– En lead er en e-postadresse, et telefonnummer eller et samtykke, sa den svenske nettmarkedsføreren Ramin Jamei, som vi kom i kontakt med i løpet av artikkelserien:

– En utvist interesse, der noen har sagt ja til å motta informasjon om å bytte for eksempel mobiltelefonoperatør eller strømselskap.

Personopplysningene samles så av markedsføringsfirmaene som står bak. Enten er de skaffet til veie på vegne av en kunde, som eksempelvis kan bestille «10 000 norske nettbrukere med interesse for nytt strømselskap». Eller de kan samles inn og lagres av nettmarkedsførerne selv, og tilbys for salg i ulike sammenhenger.

Slik startet det

Høsten 2017 gjorde en slektning av Sonja Nordanger – journalist og tillitsvalgt i Aller-konsernet, et Google-søk for å finne en bestemt artikkel Nordanger hadde skrevet. Søkeresultatet forbauset dem begge. I tillegg til de forventede treffene, som sosiale medier-profiler og artikler Nordanger hadde skrevet, dukket det opp en rekke uventede nettsider.

Disse nettsidene viste innhold fra artikler hun hadde skrevet – hos KK, Dagbladet og Vi.no. Men innholdet var stjålet og flyttet til nye nettsider. Da Nordanger klikket seg videre fra disse nettsidene ble hun videresendt til både pornosider, til suspekte annonser og «konkurranser», som eksempelvis lovet at du kunne vinne en ny telefon.

Nordanger ønsket å få de uønskede Google-treffene fjernet. Hun kontaktet derfor utviklingsavdelingen i Aller. Det viste seg at også flere andre Aller-ansatte hadde samme problem. Når de søkte på artikler ble de viklet inn i spam-sider, som hadde stjålet seriøst innhold og som fort avkrevde en personopplysninger

Utviklingsavdelingen hjalp Nordanger og de andre med å sende inn klager på hver enkelt side gjennom Googles klagesystem. Men saken pirret også nysgjerrigheten til utvikler Tor Henning Ueland, som har lang erfaring i å grave i nettkriminalitet.

Ueland begynte senhøstens 2018 å følge med på de ulike spam-sidene, og så smått undersøke domenenavn samt om det fantes forbindelser spam-sidene imellom. Uelands innledende undersøkelser bekreftet at det var snakk om et nettverk, og ikke bare noen få enkeltstående svindelsider. (se metodekapittel)

Sammen med Geir Wiksen, teknologidirektør i Aller Media, kontaktet han nyhetssjef Hans-Martin Thømt Ruud og gravesjef Siri Gedde-Dahl, og foreslo å grave videre.

Torgeir P. Krokfjord, journalist i gravegruppa i Dagbladet, tente på ideen og begynte sammen med Ueland å grave i midten av januar 2019. Ueland og Krokfjord jobbet, delvis på heltid, delvis på deltid, med prosjektet i omkring tre måneder. Artiklene ble publisert i løpet av de siste fire ukene. Siri Gedde-Dahl reportasjeledet prosjektet, i tillegg til at teknologidirektør Wiksen i perioder var tett på prosjektet da både Dagbladet og andre Aller-nettsteder også var rammet.

2. TEKNISKE METODER

Systematisering og jakt på mønstre

Som et stort mediehus får vi av og til tips om misbruk av merkevarkene våre. I forbindelse med tipset fra Sonja ble både sidene hun tipset om, samt en del tidligere tips samlet opp i et regneark. De forskjellige sidene ble også manuelt vurdert.

Det ble videre gjort Google-søk basert på innholdet vi så på de aktuelle sidene. Treffene som Google-søkene ga, ble også lagt til i regnearket.

Et eksempel på et slikt søk er: «‘er en del av Aller Media’ -site:.no -site:.com», som søker etter setningen “er en del av Aller Media” på alle nettsider som ikke ligger ligger under .no eller .com.

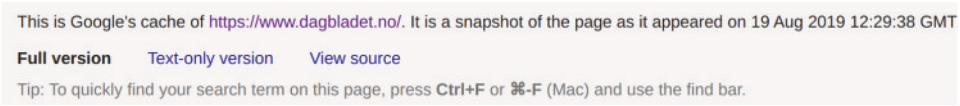
Metode: Graving i nettsider

269 forskjellige domener ble i løpet av et par uker lagt inn i regnearket, sammen med informasjon om hvor mye innhold Google hadde gjort søkbart på hvert nettsted. Dette for å se hvor mye stjålet innhold

det kunne være snakk om per nettsted. Vi la også inn informasjon om hva slags type kopi det var snakk om. Det stjålne innholdet ble enten vist frem som en ren kopi av nettstedet («siterip»), eller som et «forum», der det stjålne innholdet ble lagt inn som «diskusjoner» på forumet.

Vi undersøkte så et par tilfeldig utvalgte sider i hver kategori manuelt, for å se etter spor som vi kunne bruke videre i vår jakt på bakmennene. Sidene som ble kategorisert som «forum», ga oss ingen interessante spor eller koblinger. Men sidene som ble kategorisert som «siterip", skilte seg fort ut, og ble fokus for vårt videre arbeid.

Ved undersøkelse av kildekoden på «siterip»-sidene viste det seg at kildekoden var nesten identisk med nettsiden som var kopiert. Spamsidene skilte seg bare ut ved et par lenker til andre nettsteder, som stod helt øverst på nettsidene. Disse lenkene passet ikke inn i mønsteret med andre lenker på nettsidene. Denne listen var kun synlig i nettstedets HTML-kode. Besøkte man siden direkte i nettleser ble man sendt videre til reklame/svindel-sider. Når man så på siden via Googles bufrede kopi, ville Googles banner legge seg over denne listen.



(Eksempel på Googles banner som la seg over listen over nettsteder)

Nærmere undersøkelser av nettsidene som det ble lenket til, viste at samtlige nettsider hadde en rekke likhetstrekk:

- Alle hadde klonet et seriøst nettsted
- Alle lenket videre til andre kopierte nettsteder
- Alle brukte toppdomenenavn som gikk igjen
- Alle hadde Letsencrypt HTTPS-sertifikater
- Alle brukte leverandøren Cloudflare for å skjule sine spor.

Her så vi altså konturene av et større nettverk, og begynte å vurdere hvordan hele nettverket kunne bli avdekket.

Vi antok at målet til de som stod bak dette, var å få mest mulig innhold søkbart hos Google. Dette for å få flest mulig som gjør et Google-søk, til å trykke seg inn på sidene. Dette igjen ville da medføre trafikk til de tjenestene som de ønsket å annonsere for. Et av de viktigste kriteriene for å komme høyt på Googles søkeresultater er å ha flest mulig lenker inn til nettstedene, det var da naturlig at alle disse sidene i nettverket lenket til hverandre.

Metode: Crawler

Ettersom nettstedene i nettverket lenket seg i mellom, og dette ble brukt for å øke Googles vekting av nettverket, var dette også et fint utgangspunkt for å finne ut mer om nettverket. Ueland satte seg derfor ned og skrev en crawler (dataprogram som henter og indekserer nettsider) i Python3, med lagring i databasemotoren MySQL. Denne samlet så inn data om nettverket på følgende måte:

- Først, hent en liste over de nettsidene som skal undersøkes, besøk så den eldste i listen.
- Loggfør hvilken IP-adresse nettsteder ligger bak
- Sjekk så om det finnes lenker til andre nettsteder i toppen av nettstedets forside.

- Se om lenkene i toppen peker til et av følgende toppdomener:
    - *.cf, *.tk, *.ga og *.gq
- Hvis ja, lagre nettstedet som en mistenkt klone, og legg til en kobling mellom besøkt nettsted, og nettsted det lenkes til.
- Lagre også både forsidens tittel og forsidens HTML-kode
- Undersøk HTTPs-sertifikatet til nettstedet for å se når det ble sist oppdatert

Crawleren satt opp til å fremstå som en vanlig Chrome nettleser, samt satt til å automatisk kjøre fra en rekke servere over flere måneder. På den måten kunne vi følge med på nettverkets utvikling. Samtidig som vi ikke sendte så mye trafikk fra en enkelt IP, at det ikke skulle gå av noen alarmer på nettstedene vi overvåket.

```
    print("Fetching site...")
    request = urllib.request.Request("http://"+todo,headers=
{'User-Agent': 'Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/
537.36 (KHTML, like Gecko) Ubuntu Chromium/71.0.3578.80 Chro
me/71.0.3578.80 Safari/537.36'})
```

(Dataprogrammet går undercover under dekket av nettleseren Chrome)

Metode: Programmering

Undersøkelser i råmaterialet i MySQL-databasen viste tidlig at vi her så på materiale som var stjålet fra en rekke land. Det var derfor grunn til å tro at dette nettverket var rettet spesifikt mot disse landene. Ueland skrev derfor et program som sjekket den innsamlede HTML-koden for hvert nettsted og gjorde en vurdering av hvilket land klonen kom fra. Scriptet gjorde en ren vurdering av språket spesifisert i nettsidenes HTML-kode (html-elementets lang-attributt) i de tilfellene det var spesifisert. Dette lot oss kategorisere 37 000 av totalt 85 000 nettsteder som vi klarte å få en kopi av.

#	country	unique_sites
1	slovenia	3
2	croatia	3
3	slovakia	46
4	sweden	2203
5	denmark	2892
6	netherlands	3851
7	greece	4339
8	france	4474
9	germany	4503
10	unknown	4646
11	norway	4781
12	finland	5476

(Oversikt over hvilke land vi klarte å klassifisere innhold til)

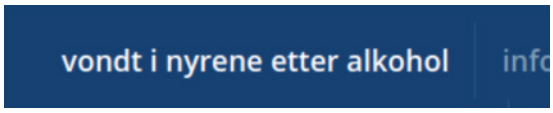
Som oversikten over viser, så var dette en kampanje klart rettet mot europeiske land. Et land som skiller seg ut her er, som vi senere skal redegjøre for, Hellas.

```
1 <!DOCTYPE HTML><!DOCTYPE html
2 <html lang="no">
3 <head>
```

For å få en oversikt over hvilke land kampanjen ble rettet mot, ble det laget et program som analyserte den innsamlede HTML-koden fra de kopierte sidene for å klassifisere hvilke land de kom fra. Dette kunne for eksempel blitt gjort ved å la Google Translate undersøke hvilket språk den tror teksten er på.

Men ettersom vi visste at innholdet ble omskrevet til setninger uten mening i mange tilfeller, ble løsningen å gå for en mer «brute force»-aktig metode. Det vil si at vi lagde et program som undersøkte

kildekoden til nettstedene og klassifiserte språk avhengig av hvilket språk som var spesifisert der.



(Eksempel på omskrivning gjort på nettsidene)

Crawleren kjørte konstant i flere måneder. Når den hadde gjennomgått hele nettverket, begynte den forfra igjen. På den måten kunne vi hele tiden holde oss ajour med nettverket og plukke opp nye nettsider etterhvert som de ble lagt til i nettverket. Ettersom HTTPS-sertifikater fra Lets Encrypt har en levetid på 3 måneder, gir det fort begrenset med informasjon å se så mye på starttidspunktet på sertifikatene. Men vi kunne blant annet se at det på en enkelt dag mellom august 2018 og januar 2019 kunne bli opprettet/fornyet sertifikater for alt fra 1 til 3000 unike nettsteder.

Som tidligere omtalt, var flere av Aller sine egne nettjenester kopiert. Men ettersom alt vi fant var plassert bak leverandøren Cloudflare, som sørger for å tilsløre koblingen til den faktiske tjenesteleverandøren, var det vanskelig å se hvilke IP-adresser som stod bak de kopierte nettsidene. Dette var ønskelig å finne ut av, både for å kunne finne ut mer om hvem som står bak, men også for å kunne blokkere kopiforsøkene.

Vår opprinnelige teori var at de som stod bak dette, hadde kopiert nettsidene rått. Men når vi begynte å undersøke trafikken mot enkelte av tjenestene våre, så oppdaget vi fort at det ikke var snakk om en ren kopi. Ved å besøke «https://www.<url-til-kopi-av-kk.no>/dette-er-en-ikke-eksisterende-side» i en nettleser, oppdaget vi samtidig i våre systemer at det ble gjort en forespørsel mot «https://www.kk.no/dette-er-en-ikke-eksisterende-side» fra en serverleverandør i Frankrike. Ved å gjøre dette mot alle svindelsidene som vi visste gikk mot nettsider i vår kontroll, satt vi igjen med flere forskjellige IP-adresser, alle pekte til samme leverandør. (Dette omtales også under presseetiske vurderinger)

Etter denne oppdagelsen kunne vi da anta at de som står bak, har satt opp en proxy-tjeneste av et slag. Proxytjenesten sender forespørsler til svindelsidene, videre til offerets nettside. For så å skrive om innholdet før det returneres til leseren.

3. JAKTEN PÅ BAKMENNENE

Den franske milliardæren

Spørsmålet var nå: Hvem var det som eide og tjente penger på det suspekte nettsystemet?

Vi søkte på IP-adressene i domenesøkeren Whois, og fant ut at IP-adressene sto registrert på «Iliad Enterprises», og at serverne deres fysisk befant seg i Paris.

Videre fremgikk det at IP-adressene tilhørte et autonomt system med kode 12876. Et autonomt system er et system av rutere som administreres sammen, og som følger en felles policy for å sende data mellom hverandre. Et autonomt system har som hovedoppgave å håndtere nettrafikk innenfor en viss del av nettet, og administreres av en bedrift eller en nettleverandør.

Det framgikk også av Whois-treffet at IP-adressens vertsnavn var rev.poneytelecom.eu.

Ved å Google både Poney Telecom og AS12876 fant vi at Poney Telecom-nettet var nevnt på en rekke

blogger og nettforumer. Vi søkte videre på stikkordene på Twitter og Facebook, og fant også der en rekke brukere som klaget på det aktuelle systemet. Stikkordene var nettopp spamvirksomhet og suspekt annonsering, – slik vi også mente det var. I tillegg mente noen av bloggerne at Poney Telecom-nettet ble brukt til dreide seg om ren nettkriminalitet, som hacking og phishing.

Vi søkte på Iliad i det franske selskapsregisteret på https://portal.kyckr.eu/, og fant ut at Iliad, Online.net, Poney Telecom og Scaleway tilhørte samme selskapskonglomerat – og var eid av en Xavier Niel.

Niel er ikke spesielt kjent i Norge, men i Frankrike er han en av landets mektigste næringslivsledere, og landets 7. rikeste mann. Niel er anerkjent som en genial IT-gründer og forretningsmann, men har også tjent penger på mer snuskete nettvirksomhet – blant annet var han en pionér innen nettporno. Nå hadde han altså tjent penger på nettangrepet mot Dagbladet, VG og en rekke andre norske medier.

Vi forsøkte gjentatte ganger å komme i kontakt med Niel og Iliad-direktør Thomas Reynaud, men fikk aldri noen svar. Iliad/Scaleways sikkerhetssjef opplyste imidlertid at selskapet skulle ta affære mot piratene etter Dagbladets henvendelse.

Niel var altså mannen som eide serverne, men hvem stod bak spamsidene?

Bakmennene avslører oss

Da prosessen med å kontakte tjenesteleverandører og kilder pågikk, hadde vi ennå ikke en klar kobling til de som stod bak. Men vi oppdaget noen dager senere at mange av nettstedene som før var klassifisert som norske nettsteder, ble klassifisert som greske nettsteder. En sjekk av en rekke av nettstedene vi hadde samlet inn, viste at de enten returnerte greske nettsteder eller var tatt helt ned. Vi antok da at bakmennene nå var kjent med jobben vår, og valgte da å stoppe overvåkingen og jobbe videre basert på de dataene vi hadde fått samlet inn.

Vi hadde da klart å samle inn:

- 1,27 millioner krysslenker mellom nettstedene
- Kopi av 85 000 nettsteder

Hjelperen «Jonas»

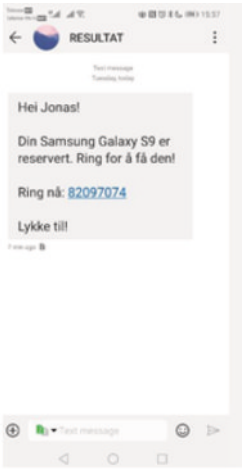
Vi visste nå hvem som eide selskapet som eide og administrerte serverne i Frankrike som ble brukt for å stjele innholdet fra tusenvis av norske og utenlandske nettsteder.

Men hvem laget annonsene og tjente penger på dem?

Når du klikket på de suspekte spam-sidene med stjålet innhold fra Dagbladet, VG, BBC, Aftenposten, NRK, Statens vegvesen, Fylkesmannen eller andre, fikk du i mange tilfeller opp det som tilsynelatende var ulike konkurranser.

Vi ønsket altså å finne ut hvem som sto bak konkurransene, og finne ut hvordan det hadde seg at de dukket opp på nettsider med stjålet innhold både fra Norges største aviser og fra viktige, offentlige nettsteder. Vi måtte på innsiden, men var lite lystne på å legge inn egne personopplysninger i systemet.

Vi lagde derfor en bruker – «Jonas» – med en anonym Hotmail-adresse, en falsk fødselsdato og postadresse i nabobygget til Dagbladet. Og egen mobiltelefon?

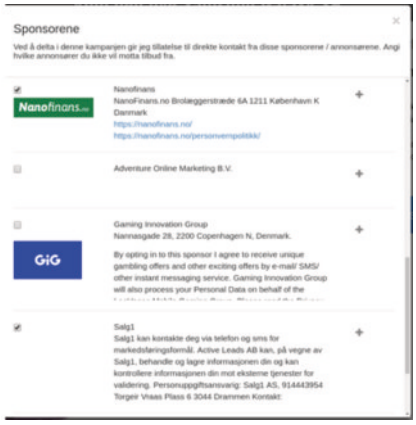


Du måtte taste inn navn, e-postadresse, fødselsnummer og gjerne opplyse betalingskortinformasjon – for å vinne en smarttelefon, få kjøpt en telefon for 1 krone eller lignende tilbud. Ved å klikke videre gjennom konkurransen og opplyse informasjon fikk du ulike nettsider opp på skjermen, og du måtte gjerne oppgi personinformasjonen din flere ganger – til flere ulike selskaper. Med personopplysningene til «Jonas» klikket vi oss fra skjermbilde til skjermbilde i flere av konkurransene. Underveis ble vi både bedt om å ringe et nummer, som ifølge den lille skriften, utløste et abonnement til 125 kroner i uka. Vi fikk også følgende sms – fra et nummer som koster 26 kroner minuttet:

«Hei Jonas!
Din Samsung Galaxy S9 er reservert. Ring for å få den!
Ring nå: 820XXXXXX
Lykke til!»

Etter hvert som «Jonas» klikket seg gjennom annonsesidene, og ga personopplysningene og e-postadressen til selskaper som fristet med både Iphone- og Samsung-telefoner, fikk vi til slutt opp en rekke med «sponsorer». For å til slutt kunne få telefonen måtte «Jonas» samtykke i å motta korrespondanse og bli kontaktet av en lang rekke selskaper, som altså sto oppført som «sponsorer» av konkurransen.

Blant disse var et kjent norsk selskap som strømgiganten Norgesenergi, i tillegg til norske selskaper som Spillselskapet GIG, som har flere norske idrettsprofiler på eiersiden, salgsfirmaet Salg1 i Drammen og en underleverandør til den norske forbrukslånskjempen Axo Finans.



Underveis tok vi screenshots av alle nye skjermbilder – inkludert URL på hver side – for at vi ikke skulle gå glipp av noe informasjon som kunne bringe oss nærmere bakmennene.

Vi kontaktet en rekke av «sponsorene» som dukket opp. De norske selskapene besvarte våre henvendelser enten med fullstendig stillhet – som GIG – eller med total, forskrekket fornektelse, som Norgesenergi og Axo Finans. Begge selskaper hevdet seg misbrukt og påsto at deres logo hadde havnet i konkurransen ved en feil.

– Dette er åpenbart en dårlig praksis, slo Axo Finans-toppsjef Carl Edvard Endresen fast overfor oss.

Hvem var det så som sto bak annonsene – som selv de norske annonsørene tok avstand fra?

Listen over sponsorer ga noen indikasjoner.

Metode: Whois-undersøkelser

Et av selskapene på lista over «sponsorer» var Zinq Media. Selskapet oppga i annonsen å være registrert i Nederland. I nederlandske selskapsregistre fant vi ut at selskapet var en del av R&D Media – et selskapskonglomerat som ifølge nederlandske medier var eid av en kontroversiell, nederlandsk gründer. Selskapsstrukturen er – ifølge nederlandske medier – knyttet både til kontroversielle sms-abonnement, udokumenterte fakturaer og «gratis» tilbud som viser seg å koste 50 euro.

Dette var altså selskaper som så ut til å drive med en virksomhet som lignet på den spam-annonseringen vi undersøkte.

En artikkel i en nederlandsk avis gjorde oss ytterligere nysgjerrig. Avisa FTM skrev at selskapene tidligere var bøtelagt en rekke ganger for sin virksomhet. Selskapene skulle ifølge FTM også tjent store penger på kjøp og salg av leads – vanlige folks navn, nummer og e-postadresser.

Kunne R&D-selskapene være bakmennene vi lette etter?

Videre graving ga flere interessante funn i så måte. På sponsorlista fant vi også selskapet Promo Selections. De oppga kontaktinformasjonen til et selskap i Malaysia: Conversion Factory, med nettstedet conversionfactory.com. Det var lite å hente om dem på nettet. Og da vi søkte i domeneregisteret Whois fant vi heller ingenting. Men siden selskapet oppga å være malaysisk, kunne det være at nettadressen var feilstavet på nettstedet vi kom over? Vi forsøkte nye Whois-søk, men la nå på endelsen «.my» for Malaysia. Da var det mer å hente. Ved å søke på conversionfactory.com.my i Whois fant vi kontaktinfo til flere personer i selskapet.

- Samtlige hadde e-postadresse som sluttet på @rdmedia.com – samme nederlandske selskapsstruktur som kunne knyttes også til andre sponsorer.

Vi skulle finne ytterligere et spor til R&D Media. En av konkurransene vi fikk opp ved å klikke på spam-annonsene oppga å være laget av selskapet Surfeyo. Konkurransen oppga ingen videre informasjon, og ved første øyekast var det heller ingen kontakt- eller registreringsinformasjon på Surfeyos nettsider. Selskapsnavnet "Surfeyo" eksisterte verken i norske, britiske eller nederlandske selskapsregistre. Men ved nøyere gjennomgang av Surfeyos nettside fant vi, nederst i personvernretningslinjene for Irland, følgende:

Conversion Factory/ Surfeyo
Dutch representative Surfeyo / The Netherlands
PO box 15748
1001 NE Amsterdam

Dermed kunne også Surfeyo spores direkte til R&D-systemet, siden vi allerede hadde avdekket at Conversion Factory lå under R&D.

Ut fra dette kunne vi slå fast at en rekke av R&D-selskapene sto som sponsor til spam-konkurransene. Men det samme gjorde jo både Norgesenergi og underleverandøren til Axo Finans, som begge hardnakket insistert på at de var blitt lurt og misbrukt. Hvordan hang dette sammen? Vi kunne ikke være sikre på om eierne av R&D-selskapene faktisk var de bakmennene vi lette etter.

Metode: Servergranskning

Både da vi undersøkte de franske IP-adressene, og da vi undersøkte selve spam-sidene, fant vi at mange av sidene/IP-adressene ble skjult ved hjelp av tjenestene til det amerikanske IT-firmaet Cloudflare.

Mange av spam-sidene hadde sin såkalte «navneserver» registrert hos selskapet Cloudflare. En navneserver oversetter domenenavnene – db.no, vg.no – til tall. Slik blir nettsteder mulig å spore på Internett. Men noen ønsker å skjule sitt egentlige opphav. Der kommer Cloudflare inn i bildet. Om du registrerer nettstedet ditt hos dem, blir det nærmest umulig å finne ut hvem du egentlig er. Det hadde nettpiratene gjort.

I research-fasen kom vi i kontakt med det amerikanske IT-selskapet Security Trails. De har laget en

oversikt over hvilke nettsider som bruker de to aktuelle Cloudflare-navneserverne.

Vi gikk igjennom registeret til Security Trails, og fant at store selskaper som Microsoft og Volkswagen brukte navneserverne. Dagbladet bruker selv tilsvarende tjenester.

Men vi fant også nettsider med kryptiske navn, tilhørende China Mobile – et kinesisk selskap som USA har stengt ute på grunn av fare for spionasje. På lista over nettsteder på navneserverne fant Dagbladet også et nettsted der adressen tydelig tilsa at nettstedet tilbød filmer som viste overgrep mot barn. Dette nettstedet omtalte vi. Kripos satt nettstedet under overvåkning, etter at vi kontaktet dem for en kommentar. Vi intervjuet Cloudflares juridiske direktør Doug Kramer – tidligere stabssekretær for president Barack Obama. Han erkjente at de ikke hadde fanget opp det aktuelle nettstedet, hvis adresse tydelig indikerte at det dreide seg om overgrepsmateriale. Kramer sa: Er nettadressen så eksplisitt som den du henviser til, er det sannsynlig at det er noe ulovlig der. Da varsler vi myndighetene.

4. GUDFEDRENE

Muntlige kilder

Hva var hensikten med å bruke stjålne avisartikler fra norske aviser til å få folk til å klikke på annonser de ikke hadde bedt om?

Samtidig som vi gravde og systematiserte ved hjelp av programmering og koding, og lette i selskapsdatabaser og nettregistre, drev vi også god gammeldags kildekontakt. Det var muntlige kilder som skulle hjelpe oss videre. Ikke minst var det muntlige kilder som ga oss svaret på hvorfor innholdet fra Dagbladet, VG og de andre faktisk hadde en verdi:

Reklamebyråene rangerer nasjonaliteter i tre kategorier, gikk det fram på bransjesider vi kom over i vår research: Etter kjøpekraft og hvor attraktive de er å annonsere i. Norge er i kategori 1, sammen med 18 andre rike i-land. Handelsvaren til selskapene vi undersøkte var som sagt såkalte «leads». En kilde som hadde bred kjennskap til lead-generering kunne opplyse at tyveri av innhold, som Dagbladet og de andre var utsatt for, var vanlig i bransjen. Intervjuet med denne kilden ble presentert slik i artikkelen:

«En kilde med god innsikt i annonsekampanjen, der det kopierte Dagbladet- og VG-innholdet er brukt, sier:

– Jeg har grunn til å tro at innholdet fra blant annet deres side er brukt til å lage det som på fagspråket kalles en «landingsside», eller en «trakt».

- *Hva vil det si?*

– Det vil si en side som skal lure kundene inn dit annonsørene vil ha dem. Kundene blir lurt til å klikke på en side med eksempelvis stjålet innhold fra en avis – hvorpå de sendes videre til annonsene som lurer i bakgrunnen.

– *Hvorfor lager man slike landingssider?*

– Min erfaring er at store lead-genereringsfirmaer ofte tar på seg oppdrag som er større enn de vet de kan klare med vanlige metoder. Da trenger de å være kreative. For eksempel slik det har skjedd i deres sak.

Vedkommende ønsket ikke navnet sitt på trykk – og vi skulle snart få vite hvorfor. Kilden ønsket nemlig å gi et hint om et navn som stadig, ifølge personen, gikk igjen i saker som den vi gravde i:

– Vil du vite hvem som er gudfedrene til denne bransjen, spurte den erfarne skandinaviske markedsføreren vi var i kontakt med, og fortsatte:

– Svaret på det er Egentic.

Spor mot Tyskland

I samme fase av researchen fikk vi også annen informasjon som skulle gjøre selskapsnavnet Egentic svært aktuelt. Vi hadde funnet R&D-selskapene, som i seg selv var interessante. Men det hadde ikke vært mulig å knytte dem til en aktiv rolle, utover å stå som sponsorer på linje med de norske selskapene.

Av en ny, anonym muntlig kilde fikk vi nå enda et hint. Vedkommende hadde nemlig innsikt i hvem som hadde solgt sponsorplassen til det lille salgsfirmaet Salg1 i Drammen – som sto oppført som sponsor sammen med Norgesenergi og de andre. Dermed kunne vi for første gang få informasjon om hvem som faktisk hadde solgt sponsorplassen, og dermed tjent penger på å selge annonseplass som var direkte linket til dataangrepet mot Dagbladet og de andre.

Salg1s daglige leder, Kenneth Burud, ønsket ikke å kommentere saken. Men via bredt kildearbeid kom vi likevel i kontakt med en person som bekreftet at det var det svenske markedsføringsselskapet Active Leads som solgte Salg1 sin sponsorplass.

Active Leads drives av samme Ramin Jamei som overfor oss hadde beskrevet bransjens arbeidsmetoder. Men Jamei og Active Leads var ikke alene om å knytte det lille salgsfirmaet Salg1 til spam-annonsene. Vi fikk opplyst at da det lille, norske selskapet Salg1 skulle betale for oppdraget til Active Leads, kom det to fakturaer i posten: En faktura fra Active Leads. Og en annen faktura fra Egentic.

Forelagt dette sa Ramin Jamei, daglig leder i Active Leads: – Vi samarbeider med Egentic på visse kampanjer.

Et Google-søk på Egentic avdekket at selskapet hadde vært knyttet til en rekke kontroversielle kampanjer i Norge tidligere. Selskapet hadde blitt knyttet til lignende dataangrep mot Coop, Expert og Get, og ble advart mot av norske forbrukermyndigheter. En rekke ganger hadde de blitt omtalt i norske medier. Men de hadde aldri svart på spørsmål, og ingen av selskapets ledere hadde blitt tvunget til å stå fram og svare for seg eller forklare selskapets metoder.

Mye tydet på at de nå var på ferde igjen.

Metode: Graving i kildekode

For å se hvor stor Egentics rolle i saken var, tok vi for oss det vi hadde mye av, nemlig suspekte nettsider.

Ved å høyreklikke på en nettside du har oppe i nettleseren, får du opp den såkalte kildekoden. Wikipedia definerer kildekode slik: «instruksjoner til en datamaskin skrevet på en form som mennesker kan lese. Kildekode må gjøres om til maskinkode for å kunne kjøres på datamaskinen. Vanligvis består kildekode av en tekstfil med instruksjoner (...)»

I kildekoden kan det stå ulik informasjon. Blant annet hvem som eier nettstedet du er inne på. Vi gikk systematisk gjennom alle konkurransene vi hadde fått opp. Og fant spor som ledet nettopp til den kontroversielle, tyske markedsføringsgiganten som norske forbrukermyndigheter hadde advart mot.

En av annonsene som gikk igjen ofte når du klikket på nettsidene med stjålet innhold, lød som følger:

«Kjære Chrome-bruker. Du er dagens heldige besøkende for [dagens dato]. Ta denne korte undersøkelsen, så vil du som takk få sjansen til å vinne [sic] Apple Iphone X!»

Svarte du på spørsmålene i den undersøkelsen, fikk du opp en ny annonse:

«Iphone X FOR BARE 18.99 NOK.»

Her må du gi fra deg ikke bare mobilnummer og e-post, men også kortnummer, utløpsdato og sikkerhetskode. Den aktuelle annonsen lå på en kryptisk nettadresse (url), med en lang rekke tall og bokstaver. Men fremst lå toppdomenet ritkunfa.info. Vi åpnet nettstedet ritkunfa.info i nettleseren og gikk inn i kildekoden: Der gikk det fram at ritkunfa.info var drevet av et selskap som het Toleadoo – og kom fra Tyskland.

Metode: Selskapssøk og sosiale medier

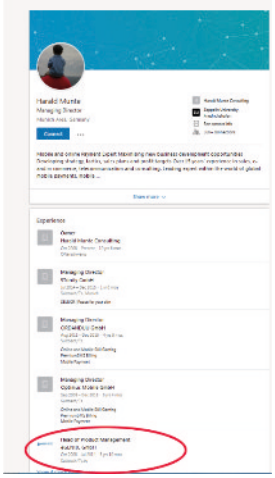
Vi søkte opp det tyske selskapsregisteret – https://www.unternehmensregister.de – på Google, og lagde en brukerkonto. Der søkte vi opp Toleadoo, og fant registreringsinformasjonen og historikken. Vi lastet ned alle dokumentene. Det samme gjorde vi med Egentic. Da oppdaget vi at Toleadoo og Egentic hadde samme adresse. I historiske dokumenter fra selskapsregisteret gikk det også fram at de to selskapene ikke bare hadde felles adresse nå, men at de også hadde flyttet fra en adresse til en annen samtidig.

Vi så at direktøren i Toleadoo var en mann som het Jürgen Böttchner. Ved å søke på ham på Google fant vi at han også bar tittelen "head of media" hos Egentic.

Egentic selv sto også oppført på aksjonæroversikten fra stiftelsesdokumentene til Toleadoo (som den gang het Trinity) i det tyske selskapsregisteret. Vi søkte opp de tidligere lederne på LinkedIn, og fant at selskapets første direktør – på det tidspunktet Toleadoo ble opprettet – samtidig var produktsjef i Egentic.

Metode: Bufrede Google-søk

Vi googlet også «ritkunfa.info», og avgrenset Google-søket til bare å gjelde norske resultater. Da fikk vi opp flere annonsekampanjer av suspekt karakter. Vi åpnet de bufrede versjonene av kampanjene ved å klikke på den lille grønne pila ved siden av Google-resultatet. Når vi så høyreklikket på nettstedet vi fikk opp og igjen trykket på «view page source» åpenbarte Toleadoo GmbH seg i underlagsmaterialet.



Vi fant Toleadoo-navnet både på annonser tilhørende noe som het Norges Premieklubb, noe som het «Vinn Gavekort Norge» og på annonser med Experts logo - som Expert/Power bekreftet overfor oss at ikke var ekte:

– Jeg kan bekrefte at vi ikke har laget eller gitt noen fullmakt til annonsen, sa administrerende direktør Anders Nilsen i Power til Dagbladet.

Dermed kunne vi dokumentere at Egentic nå var involvert i spam-annonseringen på flere måter:

- To av spam-annonsene som hyppigst kom opp på sidene med stjålet innhold, var lagd av Toleadoo – et datterselskap av Egentic.
- Egentic selv hadde fakturert Salg1, etter at Salg1 annonserte på sponsorplass på spam-konkurransene.
- Egentics søsterselskap sto også bak flere andre spam-annonser i Norge.

Metal-referansen

Vi skulle komme over enda en link til det tyske selskapet. På en annen av nettannonsene du fikk opp ved å trykke på nettsidene med stjålet innhold, sto det oppført at annonsen, som innbefattet et abonnement verdt 125 kroner i uka, var drevet av et selskap ved navn LTT Mobile Media. LTT Mobile Media var registrert i Storbritannia, sto det.

– Ta Sjansen. Vinn en Iphone 8, lokket LTT Mobile Media i annonsen.

Å «ta sjansen» innebar å registrere deg for å delta i et «ferdighetsspill» på nettet. Du måtte også betale 125 kroner i uka. Det påstås at du kan melde deg av ved å sende en sms med «STOPP» – men ved å Google det oppgitte telefonnummeret kom vi til kundetilbakemeldinger på Gule Sider som indikerte at det ikke alltid var så enkelt. Den samme konkurransen er tidligere knyttet til norsk lettlureri hos Datahjelperne. LTT Mobile Media står i britiske selskapsregistre oppført på Sebastian Sauerborn. Han jobber til daglig som revisor i selskapet St. Matthew i London – som spesialiserer seg i gunstig skatteplanlegging og skatteparadis. Ifølge avisa Die Zeit koster hans tjenester 250–300 dollar i timen.

Vi spurte Ramin Jamei – den svenske markedsføreren som har samarbeidet med Egentic, om konkurransen stammer fra dem. Kanskje, svarte han på sms. Vi tok kontakt med Sebastian Sauerborn.

– Jeg kommenterer ikke klientforhold, svarte Sauerborn i første omgang.

Men etter flere runder fikk vi nyttige opplysninger ut av ham:

– *Er Egentic din klient, Sauerborn?*
– Min klient jobber potensielt med Egentic, svarer Sebastian Sauerborn.
I en ny e-post spør Dagbladet.
– *Er Toleadoo din klient?*

Det svarte ikke Sauerborn på. Han svarte heller ikke på hvor mye han tjener på oppdraget.

Da Dagbladet spurte om å bli satt i kontakt med klienten, og om Sauerborns klient sto bak dataangrepet mot Dagbladet og VG, fikk vi etter langvarig dialog videresendt en tekst – på tysk. Der sto det at Sauerborns klient, og deres norske partner, skulle komme med en uttalelse. Noen dager seinere kommer følgende:

«Vårt firma har aldri vært involvert i noen av de svindelsakene du refererer til.

Dessverre er det andre selskaper i vårt marked som prøver å tjene penger ved hjelp av ufine markedsføringsmetoder som ligger et godt stykke inn i gråsonen. Vi er imidlertid på ingen måte tilknyttet noen av disse, og vi benytter heller ikke andre selskaper for å utføre denne type aggressiv og villedende markedsføring. (...) P.S: Sangen din «My Mysteries Unwind» er ganske kul! Vennlig hilsen LTT Mobile Media Ltd.»

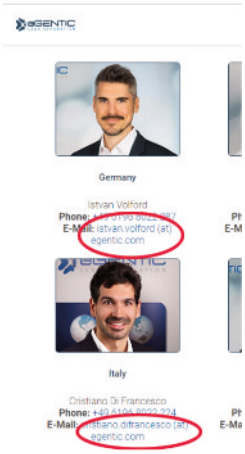
Sistnevnte referanse må forklares. Vi hadde allerede forsøkt å kontakte Egentic, på telefon og e-post, for å få selskapet til å møte til intervju. «My Mysteries Unwind» er en låt fra journalist Krokfjords tidligere metal-band. E-posten ble sendt dagen etter at Dagbladet, i en e-post der vi forsøkte å få Egentic i tale, fortalte mediesjef Jürgen Böttcher i Egentic at begge parter hadde musikk-fortid. Böttcher er nemlig trommis i den tyske delstaten Hessens svar på DDE: Rodgau Monotones (avbildet over – anbefales å sjekke på Youtube). I et forsøk på å finne tonen og finne en felles referansehorisont, skrev vi at Krokfjord også drev med musikk. Dagen etter kom en låtreferanse i retur, via revisor Sauerborn i London.

Metode: E-postleting

Egentic hadde altså vært omtalt en rekke ganger i norsk presse, men aldri svart på spørsmål. På nettsidene deres var det heller ingen kontaktinformasjon utover et sentralbordnummer, og mailadresser til enkelte selgere som åpenbart ikke var riktig adresse for spørsmål om en mediesak i Norge.

Vi ringte sentralbordnummeret, der en noe brysk dame opplyste at «Egentic ikke svarer på spørsmål». Vi spurte gjentatte ganger om å bli satt til nevnte Jürgen Böttcher – som titulerte seg som «head of media», eller til noen av selskapets tre direktører. Nei, Egentic uttaler seg ikke i pressen, var svaret vi fikk.

Det kunne være fristende å si at det var det, de hadde fått sjansen – men vi ønsket å gjøre et ordentlig forsøk til på å få selskapets ledelse i tale. Det var alvorlige opplysninger vi satt på, der både Egentic og et søsterselskap kunne knyttes til et omfattende dataangrep i Norge. Det var både av allmenn interesse, og også fair overfor Egentic, å ikke la seg stoppe av sentralborddama.



Det sto som nevnt oppført mailadressen til noen selgere på Egentics nettsider. De mailadressene ga oss formatet selskapet brukte på sine e-postadresser – som viste seg å være standardformatet fornavn.etternavn@egentic.com. Da kunne vi sende e-poster til ledelsen. Vi trengte et par forsøk på å finne riktig adresse til Böttcher – han hadde jo flere tødler i navnet sitt, som gjorde at vi måtte prøve oss fram til hvordan han formulerte navnet i e-postadressen – men etter noen feilmeldinger fikk vi avgårde e-poster både til ham og direktørene henning.munte@egentic.com, marko.reinbacher@egentic.com og hector.martinez@egentic.com. Vi sendte en rekke henvendelser til både toppledelsen og mediesjefen, og forsøkte på nytt å ringe via sentralbordet. Egentic uttaler seg ikke i pressen, ble det gjentatt – gang på gang.

Adelsmannen

I dokumentene vi hadde hentet ut fra det tyske selskapsregisteret gikk det fram at det var en mann ved navn Albrecht von Harnier som hadde grunnlagt Egentic. Seinere hadde han startet flere andre, mindre selskaper som også drev innen nettmarkedsføring og lignende bransjer. Vi googlet ham, og sperret opp øynene da vi fikk flere treff på sider som kategoriserer den europeiske adelen.

Det viste seg, rett og slett, at grunnleggeren av Egentic var adelig. Utover det tabloide poenget var det også relevant at selskapet var grunnlagt av en mann fra de øvre samfunnslag, som i utgangspunktet sto i

en maktposisjon overfor mange av dem som lot seg lure av Egentics sprell på Internett. Det motiverte oss ytterligere til å forsøke å få selskapet i tale. Vi googlet ham igjen, og fant at han en gang tidligere hadde gjort et intervju. Det var i Frankfurter Allgemeine fra 2012 – med tittelen »Datainnsamlerne fra Sulzbach» (Sulzbach er en forstad utenfor Frankfurt, der Egentic har kontor.) I artikkelen gikk det fram at von Harnier stiftet selskapet hjemme i stua si i 2001, og at Egentic i løpet av relativt få år hadde vokst voldsomt innen innsamling og behandling av data.

Albrecht von Harnier hadde, fant vi ut, et noe ambivalent forhold til å beskytte seg på nettet. Ved å søke på https://web2.cylex.de – et gratis, tysk svar på Bizweb eller Proff –v fant vi både boligadressen hans og mobilnummeret.

Men da vi så søkte på Google Maps etter adressen, fikk vi bare opp en stor sladd.

Harniers selskap var mestere i å skjule seg bak suspekte nettsider, obskure URL-er, og datterselskap. Von Harnier hadde også klart, om det var ved å gå rettens vei eller ikke vet vi ikke, å få fjernet hele huset sitt fra Google Maps.

Men å sjekke at mobilnummeret ikke dukka opp i åpne selskapsdatabaser, det hadde personverngurue glemt. Vi slo på tråden:

– *Vi jobber med en artikkel om Egentic?*
– Jeg har ikke vært involvert i driften av selskapet på 10 år.
– *Men du har fortsatt aksjer?*
– Ja, det har jeg.
– *Da du startet dette, da var det vel nesten ingen andre slike selskaper?*
– Nei, det var ingen andre. Vi var først, sier von Harnier.

Så tok han høflig avskjed. Men han ba oss også om å kontakte direktør Henning Munte om vi hadde spørsmål om aktuelle saker. Og ga oss Muntes mobilnummer. Vi hadde nå både dokumentasjon som knyttet flere spor fra dataangrepet til Egentic, og vi hadde kontaktinformasjon på både direktør og grunnlegger.

Tysklandsturen

Vi tok med oss informasjonen til Tyskland. Vi ønsket å konfrontere og fotografere både direktørene i selskapet og grunnlegger Albrecht von Harnier. Vi undersøkte først området rundt von Harniers hus, og Egentics kontorer, for å finne ut hvor vi kunne observere uten selv å bli observert – og uten å være sjenerende overfor von Harnier og hans familie, naboer, og Egentic-ansatte som ikke hadde noe med vår sak å gjøre. Vi var klar over at Egentic-gründeren hadde et barn, og ønsket ikke å fotografere verken kona eller barnet. Ved å observere biltrafikken til og fra huset og sannsynlighetsberegne rutiner ut fra dette, konkluderte vi med når det ville være lettest å få et bilde av Egentic-gründeren som var presseetisk greit å bruke, der øvrig familie ikke var i nærheten.

Taktikken fungerte, og en morgen lyktes vi å fotografere Albrecht von Harnier. Det ble første gang han var fotografert av norsk presse, etter årevis med kontroversiell annonsering i Norge. Vi valgte imidlertid bevisst å ikke konfrontere von Harnier ved samme anledning. Det var midt i morgenrushet, og sjansen for at hans kone, hans barn eller nære bekjente/naboers barn ville se konfrontasjonen var stor. Selv om vi ønsket å få ham i tale ønsket vi ikke å invadere hans privatliv i unødig grad. Heller ringte vi på døra seinere på dagen, og etterlot visittkort og en ny beskjed om hva vi ønsket å snakke med ham om (vi

hadde jo allerede snakket med ham på telefon).

Da vi reiste til Egentic-kontoret ble vi blankt avvist i resepsjonen. Der fikk vi beskjed om at vi ikke fikk snakke med noen i selskapets ledelse. Utenfor-kontoret tok vi oss da den frihet å feilparkere på en ansatt-plass med direkte utsyn mot kontorinngangen. Vi hadde på forhånd printet ut et bilde av direktørene Munte, Reinbacher og Martinez, som vi satt med foran oss i bilen. Mens vi ventet forsøkte vi på nytt å ringe Henning Munte for å avtale et intervju. På et tidspunkt fikk vi tak i ham, men han var svært avvisende:

«– Det gjelder et dataangrep mot blant annet våre nettsider – og annonser som leder fra det?
– Vi har ikke vært aktive i Norge på over et år, sier Munte.
– *Men et norsk firma ble fakturert av dere for en kampanje som stoppet i november?*
– Vi har ikke vært aktive i Norge på over et år.
(...)
– *Hadde det vært mulig å møte dere for å klargjøre hvilken rolle dere hadde i disse annonsene?*
– Det eneste du vil få fra meg er at jeg sier at vi ikke er aktive i Norge lenger. Vi gjør ikke intervjuer.
– *Hvorfor ikke?*
– Fordi vi har dårlige erfaringer med det, sier Henning Munte. – Ha det bra.»

Konfrontasjonen

Dagen etter lyktes vi omsider. Det ble nok et eksempel på hvorfor det ikke er lurt å røyke: Det var nemlig trangen etter en sigarett som gjorde at både Henning Munte og Marko Reinbacher kom ut døra og stilte seg ved siden av, rett foran bilruta vår. Vi knipset bilder, før vi gikk ut døra for å konfrontere Munte. Da la vi merke til at Albrecht von Harnier også hadde dukket opp. Han snek seg unna da vi kom – Henning Munte valgte motsatt strategi. Han nektet flere ganger for å være seg selv. Til slutt kom han etter oss for å filme. Det hele resulterte i følgende passasje på trykk:

«– Herr Munte, spør Dagbladet.
– Nei, svarer Henning Munte.
– *Er ikke du Henning Munte?*
– Nei, svarer Henning Munte.
– *Men herr Munte, vi snakket jo sammen på telefon i går?*
– Nei, svarer Henning Munte.
Så blir Henning Munte sint.
– Kom dere vekk fra denne eiendommen, snerrer han.

Vi gjør som han gir beskjed om. Så ber han om at bilder og video slettes. Det ønsket etterkommer vi ikke. Etter at vi er tilbake i leiebilen, kommer direktør Henning Munte etter, med mobiltelefonen hevet, og filmer Dagbladets team gjennom frontruta.»

I løpet av ukene før Tysklands-turen, og en rekke ganger i løpet av oppholdet i Tyskland, kontaktet vi von Harnier, Böttcher og Munte med forespørsler om å stille til intervju. Sms-er, anrop og e-poster ble ikke besvart. Likevel ble vår tur til Tyskland første gang en norsk avis lyktes med å fotografere, filme og konfrontere ledelsen og grunnleggeren av en markedsføringsgigant som i årevis hadde drevet kontroversiell virksomhet, i stor stil, i Norge.

5. PRESSEETISKE VURDERINGER

Forsøk på å stanse angrep

Det var en spesiell situasjon å drive journalistikk på et dataangrep som også rammet oss selv – Dagbladet og Aller-konsernet. Samtidig er spam-annonsering og svindel på nett et stort samfunnsproblem som rammer mange, noe som ikke minst kom fram i våre saker. Vi avdekket at bortimot samtlige store norske medier og flere statlige aktører var rammet. I tilknytning til saken hadde Allers utviklingsavdeling kontakt med Google og Nasjonal sikkerhetsmyndighet for å få stanset angrepene, som også rammet Dagbladet hardt. Dette er normale tiltak når nettsted angripes, og det ble selvsagt ikke delt noen form for kildemateriale.

Trafikksammenligning

Som hovedregel bruker Dagbladet – av personvernhensyn – ikke nettavisens trafikklogger for å sammenligne privatbrukeres aktivitet inn mot journalistiske saker. I dette tilfellet mistenkte vi imidlertid systematisk misbruk av både Dagbladet og en rekke andre store norske nettsteder. Vi mente derfor vi kunne forsvare etisk å benytte disse trafikkloggene, for å finne ut mer om hvordan misbruket foregår. Vi ønsket å stoppe misbruket. Det ble derfor valgt å kjøre trafikksammenligninger mot gitte URLer som ikke var i aktiv bruk av våre lesere.

Skjult kamera

I Vær varsom-plakaten heter det (3.10): «Skjult kamera/mikrofon eller falsk identitet skal bare brukes i unntakstilfeller. Forutsetningen må være at dette er eneste mulighet til å avdekke forhold av vesentlig samfunnsmessig betydning.»

Da vi skulle konfrontere Munte og von Harnier utenfor Egentic-kontoret valgte vi å filme seansen i skjul, med fotograf Bones' mobiltelefon. Telefonen lå i brystlomma på skjorta, mens videoopptaket gikk. Samtidig hadde vi taleopptakeren påskrudd på Krokfjords mobiltelefon. Ettersom vi var avvist i selskapet ventet vi utenfor til lederne kom ut – og konfronterte dem, med skjult kamera og mikrofon.

Det var flere grunner til at vi mente brukt av skjult kamera/mikrofon kunne forsvares:

1. Selskapet hadde over flere uker gjort alt de kunne for å unngå å svare på våre spørsmål. Vi møtte opp på hovedkontoret, ble avvist og fikk ikke snakke med noen som kunne svare på vegne av selskapet.

2. Vi hadde dokumentasjon som knyttet Egentic til alvorlige forhold. Vi ønsket å dokumentere overfor leseren at vi hadde gjort absolutt alt vi kunne for å få tak i selskapets ledelse

3. Dette var første gang noen fotograferte og konfronterte ledelsen i et svært kontroversielt selskap. Det var viktig å vise hvem de var og hvordan de møtte en konfrontasjon med sin tvilsomme virksomhet.

4. Da vi henvendte oss til Henning Munte, nektet han for at han var seg selv. Hadde vi ikke filmet opptrinnet ville det vært vanskeligere å dokumentere at vi faktisk hadde snakke med ham.

6. KONSEKVENSER

Artikkelserien har fått en rekke konsekvenser i inn- og utland:

- Nasjonal sikkerhetsmyndighet (NSM) har igangsatt full granskning, etter at statlige nettsider – som Statens Vegvesen og Fylkesmannen.no – ble angrepet. NSM har bekreftet at dette skjer på grunn av vår journalistikk.
- – Metoden som benyttes er godt kjent fra tidligere og kan benyttes til forskjellige former for svindel og lureri. Det nye er det enorme omfanget, sa Mona S. Arnøy, avdelingsdirektør i NSM.
- Vi avdekket det som trolig er et nettsted for deling av filmer som viser overgrep mot barn. Kripos satt nettstedet under overvåkning, etter at vi kontaktet dem for en kommentar.
- Google aksjonerte, og satte i sving sitt internasjonale ekspertapparat for å undersøke spam-sidene vi avdekket. Etter at Dagbladet sporet opp over 80 000 spam-sider har en rekke spam-nettsteder forsvunnet fra nettet.
- Verken VG, Fylkesmannen.no, NRK, Aftenposten, Statens Vegvesen, ABC Nyheter eller Teknisk Ukeblad kjente til at noen stjal innhold fra deres nettsteder, før Dagbladet ringte og ba om en kommentar. Samtlige tok opp saken og undersøkte forholdene etter at Dagbladet tok kontakt.
- Sikkerhetssjefen i IT-giganten Scaleway/Iliad, som eies av Frankrikes 7. rikeste mann, tok affære etter at vi oppdaget at nettpiratene brukte deres servere. Han sa: – Vi har undersøkt situasjonen du har meldt fra om. Vi har besluttet å ta ned de aktuelle serverleiene og skaffe mer informasjon om denne aktiviteten, som er forbudt hos oss og i vårt nettverk (...)

VEDLEGG: LENKER TIL PUBLISERTE SAKER I PROSJEKTET

Alle sakene er samlet her: https://www.dagbladet.no/emne/datamysteriet

Dato	Tittel	Lenke
15. mars 2019	Sonjas (52) oppdagelse avslørte det norske nettangrepet	http://db.no/70782498
15. mars 2019	Stjeler navn og nummer: Selskaper vet om du er gift, singel - eller utro	http://db.no/70782519
17. mars 2019	Google til aksjon etter Dagbladet-avsløring	http://db.no/70764373
1. april 2019	Angrepet av nettpiratene: - Kritisk for små firmaer	http://db.no/70902766
2. april 2019	Flere spor fra dataangrepet leder til tysk adelsmann	http://db.no/70890409
4. april 2019	Nettpiratene skjulte seg hos mangemilliardær	http://db.no/70793739
7. april 2019	Fant overgrepsmateriale og påstått spionselskap	http://db.no/70820893
8. april 2019	Slik unngår du å bli lurt	http://db.no/70798200
8. april 2019	Nasjonal sikkerhetsmyndighet aksjonerer etter Dagbladet-avsløring	http://db.no/70939945
10. april 2019	Katt og mus med nettpiratene	http://db.no/70825347
10. april 2019	Kripos overvåker nettside etter Dagbladet-avsløring	http://db.no/70952806