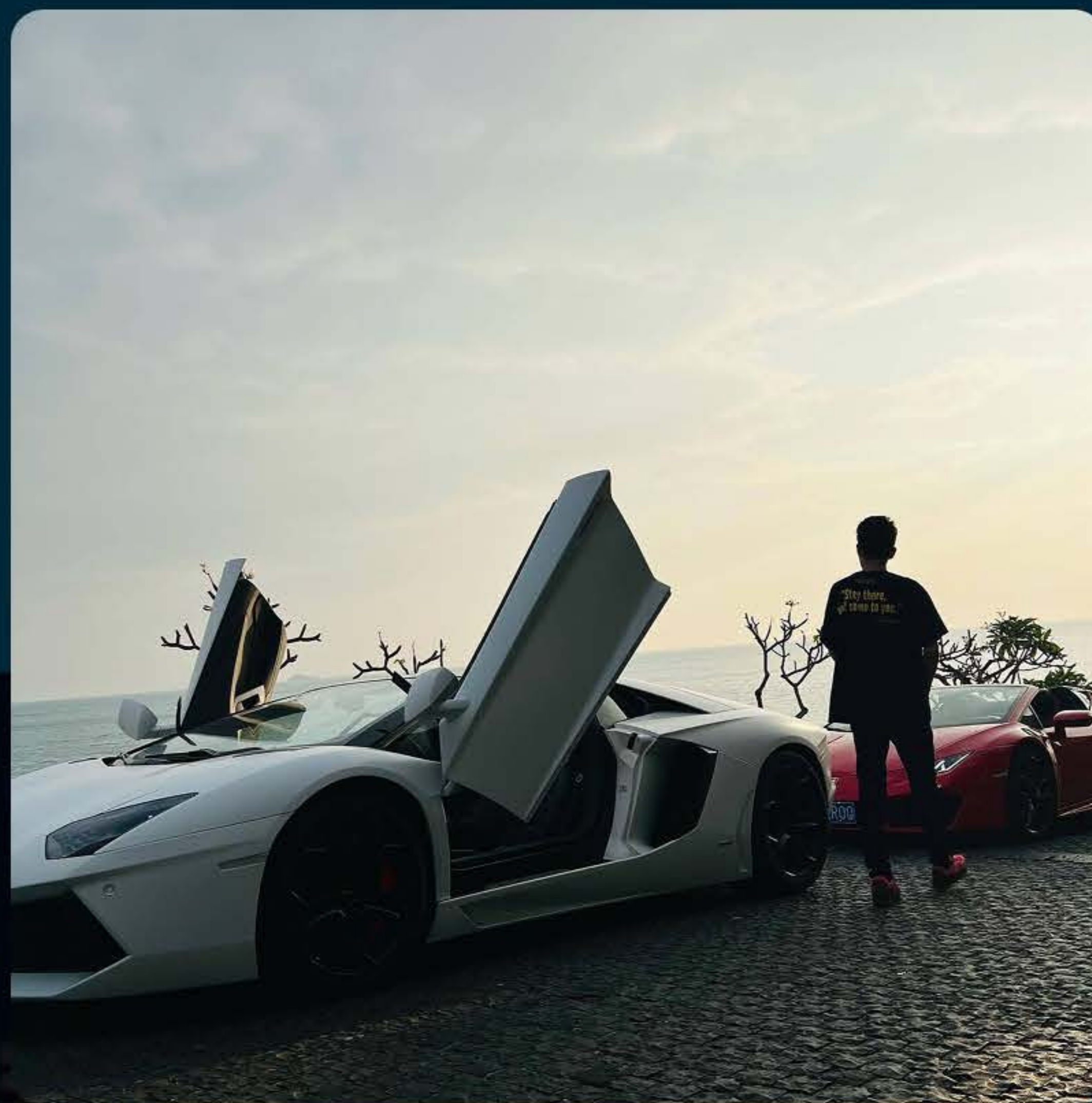


# Svindelsentralen



METODERAPPORT SKUP 2025

OSLO, JANUAR 2026



### Innsendere

Martin Gundersen

[martin.gundersen@nrk.no](mailto:martin.gundersen@nrk.no)

+47 477 56 515

Johanna Magdalena Husebye

[johanna.magdalena.husebye@nrk.no](mailto:johanna.magdalena.husebye@nrk.no)

+47 938 94 283

Jonas Alsaker Vikan

[jonas.alsaker.vikan@nrk.no](mailto:jonas.alsaker.vikan@nrk.no)

+47 928 28 316

Øyvind Gustavsen

[oyvind.gustavsen@nrk.no](mailto:oyvind.gustavsen@nrk.no)

+47 938 86 788

Henrik Løvfaldli

[henrik.lofaldli@nrk.no](mailto:henrik.lofaldli@nrk.no)

+47 902 42 739

Vicky Schaubert

[vicky.schaubert@nrk.no](mailto:vicky.schaubert@nrk.no)

+47 926 33 119

### En ekstra takk til

NRKs utvikler Vilde Jølstad Paschen og grafiker André Håker, samarbeidspartnere i den franske avisen Le Monde og den tyske allmennkringkasteren Bayrischer Rundfunk, gode kolleger i NRK som har delt erfaringer og ekspertise og, ikke minst, alle kildene.

### Publisert

Fra 4. mai 2025, prosjektet er pågående.

### Redaksjonene

NRKbeta, NRK Fakta og Gravegruppen Midt

Adresse: NRK, FG 22, 0340 Oslo

### Reportasjeledere

Ståle Hansen

Petter Moen Nilsen

### Kontaktperson

Ståle Hansen

[stale.hansen@nrk.no](mailto:stale.hansen@nrk.no)

+47 905 92 321

<b>1. Innledning</b>	<b>3</b>
1.1 Svindlernes verden	3
1.2 Slik oppsto prosjektet	3
1.3 Organisering av arbeidet	3
<b>2. Datasett og analyse</b>	<b>4</b>
2.1 Utforske Magic Cat med Google Translate	4
2.2 Spørringer via Python	4
2.3 Luhns algoritme – slik identifiserte vi de ekte kortnumrene	4
2.4 Koble kort og bank	5
2.5 Sporing av svindeltransaksjoner	5
<b>3. Telegram</b>	<b>6</b>
3.1 Falske navn på Telegram	6
3.2 Lagring av Telegram-grupper	6
3.3 Oversetting av 40.000 kinesiske chatmeldinger	6
3.4 Kategorisere spor og opplysninger	7
<b>4. De norske ofrene</b>	<b>7</b>
4.1 Møtet med svindelskam	7
4.2 Sentralbord-sjekken	8
4.3 Kode-sjekken	8
<b>5. På innsiden av Magic Cat</b>	<b>9</b>
5.1 Vi «svindlet» hverandre	9
5.2 Svindeldemonstrasjon til bank og myndigheter	9
5.3 Kjøpe lisens til Magic Cat	9
<b>6. Åpent kildesøk</b>	<b>9</b>
6.1 Søk på Line Messenger og fikser i Thailand	9
6.2 Omvendt bildesøk – og det som gikk galt	10
6.3 Kvinnens Instagram-følgere	10
6.4. Sammenligne bilder fra Telegram med Instagram og TikTok	11
6.5 Instagram-kartlegging	11
6.6 Bruk av KI-assistent og råd fra gullsmed	12
6.7 Stedsverifisering av bilder	12
<b>7. Infiltrasjon</b>	<b>13</b>
7.1 Svindelkurs og etiske rammer	13
7.2 Forberedelser og teknisk oppsett	13
7.3 Mobilinnsamling og uthaling av tid	13
7.4 Bankkort-testing og svenske banker	14
7.5 Gamingmetoden	14
7.6 Digitale og fysiske metoder smelter sammen	15
<b>8. Reportasjereise til Bangkok</b>	<b>15</b>
8.1 Fra butikkdør til butikkdør	15

8.2 Telegram-bot	15
8.3 Fra bardisk til bardisk	15
8.4 Konfrontasjon med Ken og Kris	15
8.5 Konfrontasjon med x66	16
<b>9. Jakten på Darcula</b>	<b>16</b>
9.1 Dialog med eksperter	16
9.2 Metadata fra Telegram	16
9.3 Søk på digitale identifikatorer	17
9.4. Flytdiagram til å strukturere og vekte funn	17
9.5 Slik fikk vi et kinesisk ID-kort	17
9.6 Samtidig imøtegåelse med Darcula	17
<b>10. Kinesiske hvitvaskere i Norge</b>	<b>18</b>
<b>11. Historiefortelling</b>	<b>18</b>
<b>12. Spesielle erfaringer</b>	<b>19</b>
<b>13. Motstand</b>	<b>19</b>
<b>14. Etikk</b>	<b>19</b>
14.1 Bruk av falsk identitet	19
14.2 Betaling til svindlerne	20
14.3 Identifisering av svindlerne	20
<b>15. Dette er nytt</b>	<b>20</b>
<b>16. Konsekvenser</b>	<b>21</b>

# 1. Innledning

## 1.1 Svindlernes verden

Se for deg bunkevis med stjålne tusenlapper, stablet oppå hverandre, som et tårn. Høyde: 120 meter. Samlet verdi: 1,2 milliarder kroner. Så mye svindlet kriminelle til seg fra nordmenn i 2024, ifølge [Finanstilsynet](#).

Digital massesvindler er en unik form for kriminalitet ved at den rettes mot hele befolkningen. Vi bombarderes med svindelmeldinger fra ansiktsløse kriminelle. Svindlerne kan nå alle med en smarttelefon, uansett hvor de befinner seg. Mange har nok lurt på det samme som oss: Hvem står egentlig bak svindelmeldingene?

I 2023 undersøkte en israelsk sikkerhetsforsker [tekniske spor fra en slik melding](#). Den kom fra noe eller noen som kalte seg *Darcula*. Året etter [fortalte selskapet Netcraft](#) at Darcula angrep 100 land, mens hjemme i Norge [advarte Telenor folk mot Darcula](#).

Men ingen kunne fortelle hvem Darcula var.

NRK har jaktet på ham og andre svindlere i over et år. Vi har under falsk identitet utgitt oss for å være en fersk svindler med behov for hjelp, og deltatt på svindelkurs i fire uker. Vi har infiltrert svindelgrupper på Telegram, og skrudd fra hverandre og rekonstruert svindleres eget supervåpen: Dataprogrammet Magic Cat. Dette har gitt oss en unik innsikt i svindlernes verden.

Prosjektets mål var å gi svindlerne et ansikt og finne ut hvordan de klarer å lure så mange av oss. Underveis måtte vi navigere i en jungel av stjålne kort, raske biler, kattebilder og luksusmerket Louis Vuitton.

## 1.2 Slik oppsto prosjektet

Langvarig kildearbeid i det norske datasikkerhetsmiljøet førte til at vi tidlig i 2024 mottok et spennende tips om meldingssvindler. En ansatt i sikkerhetsselskapet Mnemonic fortalte at de hadde fått tilgang til unik informasjon om et dataprogram for svindel, som het Magic Cat. NRK fikk en kopi av programmet, noen chatter mellom svindlere som brukte det, samt et interessant datasett om mulige svindelofre. Etter innledende undersøkelser av dette råmaterialet, besluttet vi å satse på dette som et graveprosjekt.

## 1.3 Organisering av arbeidet

Svindelsentralen har vært et samarbeid mellom tre redaksjoner i NRK. Halve teamet har hatt ansvar for jakt på svindlere, mens den andre delen hadde ansvar for svindelofre og manusarbeid.

Datasettet vi fikk inneholdt tall om mulige svindelofre over nesten hele verden. Mot slutten av prosjektet delte vi dataene med journalister vi kjente fra før, i den franske avisen Le Monde og hos den tyske allmennkringkasteren Bayerischer Rundfunk. Hensikten var at de kunne lage journalistikk om meldingssvindel i sine respektive land og bidra med egne funn. Vi holdt dialog på Signal.

## **2. Datasett og analyse**

### **2.1 Utforske Magic Cat med Google Translate**

Å sitte med en kopi av dataprogrammet Magic Cat, som svindlere bruker til å lure folk fra hele verden, var en spesiell opplevelse. Magic Cat fungerer bare når lisensen er betalt, men vi kunne likevel utforske layout, oppsett og innstillinger i kopien vi satt på. Språket var kinesisk. For å forstå hva som sto brukte vi appen Google Translate sammen med kameraet på en smarttelefon, og nettleser-utvidelsen til Google Translates sanntidsoversetting. Det fungerte.

Magic Cat inneholdt ferdiglagde falske nettsider for land i hele verden, som man kom til ved å trykke på lenken i en luremelding. Hensikten var å lure folk til å oppgi personlige opplysninger, kortdetaljer og en aktiveringskode. Med denne koden kunne svindlerne legge kortet til i en digital lommebok på sin egen telefon, og handle uten pin-kode.

### **2.2 Spøringer via Python**

Datasettet NRK fikk besto av opplysninger som svindlerne hadde fisket inn fra ofre i hele verden gjennom syv måneder. Det besto av totalt 13,1 millioner rader. Hver rad representerte én person som var blitt lurt, ett eller annet sted i verden. For å forstå tallmaterialet bedre, benyttet vi programmeringsspråket Python med kodebibliotekene SQLite3 og Pandas.

Slik kunne vi gjøre spøringer som ga svar på våre spørsmål. For eksempel: Hvor mange mennesker var blitt lurt til å trykke på lenken per land? Hvor mange la igjen kortdetaljer? Vi samlet analysen i en PDF-rapport med grafer og funn, som kunne leses av hele teamet. Dette sikret en felles forståelse av datasettet.

### **2.3 Luhns algoritme – slik identifiserte vi de ekte kortnumrene**

Python-spørningen viste at svindlerne hadde samlet inn totalt 959.000 kortnumre på syv måneder. Vi syntes det var et høyt tall og ville undersøke om det kunne stemme. Og heldigvis – fra studiedagene husket en av oss en egnet metode for å verifisere om et kortnummer er ekte: Luhns algoritme.

Kortnumre følger et standardisert oppsett, der de første seks til åtte sifrene angir kortutsteder (bank eller lignende). Dette kalles IIN/BIN og står for issuer/bank identification number. Det siste sifferet på et kort er et kontrollsiffer. Tallet utledes ved hjelp av Luhns algoritme, en matematisk utregning basert på de foregående sifrene.

Vi kjørte algoritmen på alle de 959.000 kortnumrene i databasen ved å bruke dette Python-biblioteket: <https://pypi.org/project/luhncheck/>.

32.000 kort besto ikke Luhn-testen eller oppfylte ikke krav til antall sifre i et typisk kortnummer, og var derfor ikke reelle. Slik fikk vi verifisert at det var 927.000 kortnummer fra hele verden som var reelle.

Vi stilte også som krav at kortnummeret skulle ha en gyldig cvv-kode, noe som normalt trengs for å gjennomføre et kjøp. Da sto vi igjen med totalt 884.000 kort globalt.

For å finne hvor mange av disse som var fra Norge, filtrerte vi på land i datasettet og fant ut at det var rundt 19.000 norske kort.

## 2.4 Koble kort og bank

Neste steg var å få identifisert hvilken bank de norske kortene hørte til. Dette gjorde vi for å undersøke om enkelte banker var spesielt utsatt for svindel.

Vi fant ingen helhetlig, offentlig tilgjengelig liste over IIN/BIN, men til gjengjeld fant vi en tjeneste som lot oss slå opp numre vi hadde i datasettet vårt: [IIN/BIN Search](#).

Vi slo manuelt opp de 100 norske IIN/BIN det var flest av i datasettet. Til slutt satt vi igjen med navn på utsteder og banker som dekket de aller fleste norske kort i datasettet. På Finans Norges nettsider fant vi en oversikt over de store bankenes markedsandel. Så sammenlignet vi denne andelen med bankenes andeler av svindelofre i datasettet. De store bankenes markedsandeler matchet i hovedsak andelen svindelofre. Altså var det ingen bank-versting blant de største aktørene. Svindelen hadde rammet svært bredt.

## 2.5 Sporing av svindeltransaksjoner

Etter å ha brukt Luhns algoritme og IIN/BIN til å identifisere banker i datasettet, gikk vi i dialog med Sparebank1 SMN i Midt-Norge. Banken aksepterte å sjekke dataene mot sine systemer og svare på våre spørsmål om hva de fant. De fant mistenkelige transaksjoner, både store og små, på svært mange av kortene i vårt datasett. Banken aksepterte å gi oss et anonymisert regneark over disse transaksjonene, med beløp og navn på butikker/nettbutikker hvor betalingen var registrert.

Dette kunne fortelle oss hva svindlerne brukte penger på – og hvor raskt de kunne slå til. Et av kortene til et svindeloffer ble belastet hele tolv ganger på ti minutter. 50.000 kroner forsvant. Vi kunne også se mistenkelige transaksjoner fra selskaper som kinesiske AliExpress og flyselskapet Cathay Pacific i Hongkong.

Men hvem var svindlerne egentlig? I datasettet sto aliaset til over 600 svindlere, som hadde kjøpt lisens til Magic Cat i perioden dataene dekket. Dette var altså en skurkeliste, som skulle bli nyttig da vi så nærmere på meldingsplattformen hvor de møttes i lukkede grupper for å diskutere strategier: Telegram.

## 3. Telegram

### 3.1 Falske navn på Telegram

Chattene mellom svindlerne (se punkt 1.2) stammet fra en lukket Telegram-gruppe for meldingssvindel. Vi ville ha tilgang til lignende grupper. Etter grundig etisk vurdering, opprettet vi profiler under falskt navn. Vurderingen utdypes i kapittel 14 om etikk.

Ved å søke på ord som typisk brukes av svindlere, som «CVV», fant vi flere grupper der Magic Cat ble promotert. Lenker som svindlerne selv delte i sine profiler ledet oss til flere slike grupper. Ved hjelp av de falske profilene kunne vi følge med på diskusjoner og aktiviteter måned etter måned. Vi postet ikke noe selv og var i all hovedsak observatører.

Noen grupper hadde tusenvis av medlemmer og titusenvise av meldinger, samt videoer av at de svindlet andre, eller bilder av varer kjøpt med stjålne penger.

Med et så stort materiale måtte vi ta et avgjørende veivalg. Hvem eller hva skulle vi fokusere på? Etter innledende undersøkelser valgte vi to Telegram-brukere som skilte seg ut:

- @darcula fremsto som en sentral IT-utvikler og administrator. Han ga datasupport om Magic Cat, men holdt ellers en lav profil. Kunne han være mesterhjernen bak supervåpenet?
- @x667788x var svært aktiv i miljøet og delte mye fra egen svindelvirksomhet. I tillegg solgte han Magic Cat og tilbød opplæring. Kunne det være avslørende detaljer i bildene og videoene han la ut?

Disse to kunne trolig kaste lys over hvordan svindelen var bygd opp (Darcula) og hvordan den ble gjennomført (x667788x – heretter kalt x66). Vi bestemte oss derfor for å jobbe med å avdekke identiteten til disse to skikkelsene i det videre arbeidet.

### 3.2 Lagring av Telegram-grupper

For å få oversikt over Telegram-materialet, måtte vi få lastet det ned og sikret det mot sletting. Deretter kunne vi analysere det offline. Vi testet flere verktøy og landet på et program kalt [tg-archive](#), som gir alle meldingene en unik ID. Dette gjorde det lett å sortere og finne frem i alt materialet. Vi lagret innhold fra sju sentrale Telegram-grupper. Det var totalt over 40.000 chat-meldinger, samt bilder, videoer og andre filer. Nå var det bare et problem: Alt var på kinesisk.

### 3.3 Oversetting av 40.000 kinesiske chatmeldinger

Omfanget av meldinger var altfor massivt til å oversettes manuelt. NRK har bedriftstilgang til [Microsofts Azure Translator v3.0 API](#). Dette ga oss mulighet til å oversette store volum av tekst.

Tg-archive lagret alle meldinger i en database. Vi åpnet databasen med Python og fikk en representasjon av databasen ved bruk av Pandas-biblioteket. Med et API kan man sende en forespørsel og få et svar tilbake. For hver chat-melding sendte vi en forespørsel om å oversette den fra kinesisk til engelsk. Vi valgte engelsk for å få best mulig kvalitet på oversettelsen. Etter noen måneder gjentok vi prosessen, for å sikre oss de nyeste chattmeldingene. Slik kunne vi lese chat-meldingene og se etter identifiserende opplysninger i dem, samt i bilder og videoer.

I svindelprosjektet har vi også jevnlig fått oversettelseshjelp av en kinesiskspråklig kollega. Mange av formuleringene i Telegram-gruppene inneholdt slang og fraser som ikke umiddelbart ga mening gjennom en maskinoversettelse.

### 3.4 Kategorisere spor og opplysninger

Nå begynte jobben med å identifisere det mest interessante knyttet til våre prioriterte mål; x66 og Darcula. I et regneark logget vi alle chatmeldinger som sa noe om:

Spesifikke steder svindlerne var	Svindelmetodikk	Norge	Opplysninger om x66 eller Darcula
----------------------------------	-----------------	-------	-----------------------------------

Til slutt satt vi igjen med nærmere 250 chatmeldinger.

Vi kategoriserte også omkring 3.000 mediefiler, som besto av memes, bilder og videoer. Relevante filer ble lagret i mapper etter kategorier, som profilbilder, bilder av klær, smykker, steder, kjøretøy og mulige boliger. Dette fungerte som dokumentasjon på svindlernes livsstil, arbeidsmetoder og som spor i den videre jakten på svindlerne.

Parallelt med at vi jaktet på svindlernes identitet, hadde vi gjennom analysen av databasen funnet tusenvis av nordmenn som var blitt lurt via Magic Cat. Nå ville vi forsøke å snakke med så mange vi kunne.

## 4. De norske ofrene

### 4.1 Møtet med *svindelskam*

Vår hypotese var at svindlerne hadde prioritert å stjele fra nordmenn som var lurt til å oppgi en aktiveringskode for å legge kortet til en digital lommebok. Av rundt 19.000 nordmenn som i løpet av syv måneder hadde blitt lurt gjennom Magic Cat, hadde over to tusen gitt fra seg koden, ifølge vår analyse av datasettet. Vi ville snakke med dem for faktakontroll og for å vise hvordan svindel rammet helt vanlige folk.

Datasettet inneholdt navn, adresser og telefonnumre. Vi tok innledende stikkprøver ved å søke på nummeropplysningstjenester som 1881.no, for å sjekke om opplysningene stemte overens. Det gjorde de.

Før vi ringte, stilte vi oss spørsmålet: Visste svindelofrene at de var blitt lurt? Det var ikke sikkert. Vi ville ikke skremme dem, men måtte være åpne om vårt prosjekt. Vi brukte følgende innledning: *«Dette kommer litt ut av det blå, men vi har fått tilgang til en liste som svindlere selv har satt opp, over hvem de har lurt. Navnet ditt er ett av tusenvis av navn på listen.»*

Gjennom de første samtalene forsto vi at mange var flau og skammet seg over å ha blitt lurt. Vi har i andre prosjekter intervjuet mennesker som har blitt utsatt for misbruk, vold og overgrep, men det var faktisk vanskeligere å få svindelofre i tale. Dette overrasket oss. Mange nektet for at de var lurt, til tross for at deres korrekte navn, adresse og kortdetaljer sto på svindlernes liste. Derfor brukte vi lang tid på å bygge tillit og finne noen som ville la seg intervju. I løpet av en måned ringte vi totalt 259 personer, og fikk snakket med 140. Kun én stilte med navn og bilde.

#### **4.2 Sentralbord-sjekken**

Noen kilder var ekstra mistenksomme da vi ringte og tvilte på om vi virkelig var NRK-journalister. Derfor la vi en strategi: Vi tilbød dem å ringe NRKs sentralbord og spørre om vi jobbet som journalister. Sentralbordet var informert om strategien, slik at de kunne bekrefte våre navn. Vi oppfordret også dem vi ringte til å søke opp i telefonkataloger på nett det nummeret vi ringte fra, så de kunne se at det tilhørte NRK. Til noen sendte vi også e-post fra vår NRK-adresse med lenker til tidligere saker, med bilde-byline. Disse grepene beroliget folk og åpnet for videre dialog.

#### **4.3 Kode-sjekken**

Før vi kunne bruke noen som case i sakene våre, måtte vi være sikre på at de var svindlet av Magic Cat-nettverket. Vi verifiserte dette ved å sammenligne aktiveringskoden svindelofre hadde fått på sms fra banken sin med aktiveringskoden som fantes i datasettet vårt. Dersom både koden, dato og tidspunkt for meldingen stemte overens, kunne vi være trygge på at svindelen stammet fra Magic Cat.

I ett tilfelle hadde mannen som var blitt svindlet slettet sms-en med koden fra banken. Vi kontaktet da banken hans og ba dem sjekke om de hadde sendt mannen en aktiveringskode til Google Pay eller Apple Pay på datoen vi hadde i vårt datasett. Mannen ga samtykke til at banken kunne opplyse om dette til NRK. Banken ville imidlertid ikke bekrefte koden til oss, men gjorde det overfor kunden. Slik fikk vi bekræftelsen vi trengte. Dermed kunne vi bruke denne personen som case.

Nå som vi hadde fått svindelofre i tale, ville vi se under panseret på Magic Cat, svindleres supervåpen.

## 5. På innsiden av Magic Cat

### 5.1 Vi «svindlet» hverandre

Vi brukte Magic Cat til å liksom-svindle hverandre og tok skjermopptak underveis. En journalist styrte Magic Cat som svindler, og trykket på de riktige knappene. En kollega spilte svindeloffer på mobil og fulgte alle stegene på den falske nettsiden, inkludert å oppgi aktiveringskoden. Denne øvelsen var avgjørende for å kunne lage en tydelig steg-for-steg-forklaring i hovedsaken.

Slik kunne NRK for første gang fortelle hvordan massesvindelen fungerer, fra tekstmelding til kapring av bankkort. Dette var viktig for å forebygge svindel i befolkningen.

### 5.2 Svindeldemonstrasjon til bank og myndigheter

Før publisering valgte vi å demonstrere Magic Cat for henholdsvis en bankansatt svindeljeger og digitaliseringsminister Karianne Tung (Ap). Vi ville observere deres vurderinger og reaksjoner. Metoden fungerte bra – og var enklere enn om vi muntlig skulle forsøkt å beskrive hvordan programmet fungerer. Statsrådets respons var overraskelse og forundring, mens den bankansatte svindeljegeren utbrøt: «Åh, er det sånn det fungerer?».

### 5.3 Kjøpe lisens til Magic Cat

Ved å være med i svindelgruppene på Telegram, oppdaget vi at det ble lansert en ny versjon av Magic Cat. Vi drøftet med redaktør, og fikk tillatelse til å kjøpe lisens i en uke. (Vi utdyper dette i kapittel 14). Med den nye versjonen av Magic Cat, kunne vi se hva som var endret og hvordan svindelmarkedet utviklet seg.

Kjøpet bidro også til å bygge troverdigheten til vår falske Telegram-profil. Ved å legge penger på bordet, fremsto profilen som genuint interessert i å lære mer om phishing. Vi valgte å kjøpe lisensen via x66, som vi holdt på å undersøke og ønsket å få et nærere forhold til.

## 6 Åpent kildesøk

### 6.1 Søk på Line Messenger og fikser i Thailand

Etter å ha gått gjennom tusenvis av bilder og videoer fra Telegram-gruppene (se punkt 3.4), satt vi igjen med noen hundre som var særlig interessante. Nå gikk vi nøye gjennom dem. Omsider kom gjennombruddet.

I et par sekunder av et videoklipp var det mulig å se at x66 var innlogget på Telegram med et thailandsk mobilnummer. Vanligvis sladdet eller skjulte han all slik informasjon, men denne gangen hadde han slurvet.

Søk på telefonnummeret ga ingen treff før vi engasjerte en fikser i Thailand. På oppdrag fra NRK gjorde hun søk på flere lokale tjenester, deriblant meldingsappen Line, som vi ikke hadde hørt om før. Der fant hun at telefonnummeret var knyttet til en profil med visningsnavnet «Kris».

Fikseren fikk en venn til å sende en venneforespørsel, noe som ga oss profilbildet til Kris i høyere oppløsning. Det viste en mann som satt i en bil med stjernehimel i taket. (Se vedlegg, figur 1)

Visningsnavnet Kris var for generelt til å identifisere andre brukerkontoer, så vi måtte bruke profilbildet for å komme videre.

## **6.2 Omvendt bildesøk – og det som gikk galt**

Men i stedet for å komme videre ved hjelp av bildet, endte vi med en lang bomtur. Vi brukte omvendt bildesøk med Google Images og fant det samme bildet hos en profil på Instagram. Innleggene på profilen viste en ung mann som oppholdt seg i Kina og Canada. Livsstilen minnet om skrytebildene vi hadde sett svindlere dele på Telegram. Kunne dette være vår mann?

På et tidspunkt bestilte vi kjøretøyopplysninger fra Canada og undersøkte eierforhold for en hundepark i Vancouver. Men etter to måneders leting hadde vi ikke funnet flere sikre koblinger mellom profilene enn et identisk profilbilde. Da vi registrerte at Instagram-profilen advarte om at andre misbrakte hans bilder på sosiale medier, mente vi det var sannsynlig at bildet var stjålet. Senere i prosjektet kunne vi konstatere at vår antakelse om bildetyveri var rett. Til slutt fant vi nemlig den riktige Instagram-profilen tilknyttet x66.

## **6.3 Kvinnens Instagram-følgere**

Med den tunge erkjennelsen at vi hadde fulgt et blindspor, gikk vi gjennom bildene som x66 hadde delt på Telegram en gang til. Der fant vi et skjermbilde fra en Instagram-samtale mellom x66 og en ung thailandsk kvinne. I tillegg var det publisert to andre bilder, som viste nyhetsfeeden til en Instagram-bruker.

Ved å se disse tre bildene i sammenheng klarte vi å finne brukernavnet på kvinnen x66 hadde sendt meldinger til. Vi kunne også se to andre profiler x66 sannsynligvis fulgte på Instagram med sin personlige profil. Alle disse profilene hadde mer enn 100.000 følgere. Det var altfor tidkrevende å se igjennom alle.

Vi bestemte oss derfor for å scrolle gjennom listen av alle kontoer de fulgte på Instagram. Det var langt færre. Hos én av disse kontoene så vi et profilbilde vi hadde sett tidligere på Line Messenger: En ung mann i en bil med stjernehimel i taket.

I tillegg til profilbildet var det flere detaljer som indikerte at dette var den personlige Instagram-kontoen til x66: Vedkommende hadde «Kris» som visningsnavn på profilen, det samme navnet som profilen på Line Messenger hadde. Han fulgte også

kvinnen som vi visste x66 hadde dialog med, og hadde et kinesisk og et thailandsk flagg synlig ved siden av navnet sitt.

Denne kontoen hadde vi ikke klart å finne uten en manuell gjennomgang av følgerlisten til den ene kvinnen, fordi selve Instagram-brukernavnet ikke inneholdt navnet Kris.

#### **6.4. Sammenligne bilder fra Telegram med Instagram og TikTok**

Da vi gikk gjennom bildene på Instagram-kontoen til Kris, ga bildene vi tidligere hadde kategorisert fra Telegram ny mening: På Instagram hadde Kris delt et bilde fra inngangen til en fin restaurant i Bangkok. Samme dato hadde x66 delt et identisk bilde på Telegram. Også et bilde fra innsiden av restauranten var delt av begge kontoene på samme dato. I tillegg fant vi nesten like bilder av raske biler, både på Instagram og i Telegram-gruppen (Se vedlegg, figur 2.)

Likhetene tydet på at vi hadde funnet svindleren x66 sin «sivile» identitet. Telegram så ut til å være der vedkommende opptredte i sin kriminelle virksomhet, mens Instagramkontoen var for det sivile livet.

Vi sjekket om brukernavnet på Instagram ble brukt andre steder. Da fikk vi et nytt treff på TikTok. TikTok-kontoen hadde publisert videoer med detaljer som matchet bilder fra x66. Blant annet kunne vi se et karakteristisk klistremerke vi tidligere hadde sett bak på x66s mobil. En annen gjenganger var en eksklusiv Louis Vuitton-jakke med et spesielt mønster. (Se vedlegg, bilder 1 og 2.)

#### **6.5 Instagram-kartlegging**

Etter å ha funnet Instagram- og TikTok-kontoene, ville vi undersøke omgangskretsen til Kris. Kanskje det var flere svindlere der? Vi tok utgangspunkt i følgerlisten hans på Instagram. Etersom ingen skrapeverktøy basert på åpen kildekode fungerte for plattformen akkurat da, «scrollet» en journalist gjennom en hel følger-liste og kopierte så ut kildekoden. En selvskrevet Python-kode hentet ut alle brukernavn som Instagram-kontoen fulgte, eller ble fulgt av.

På denne måten kunne vi differensiere mellom kontoer som gjensidig fulgte hverandre (sterk relasjon), og kontoer hvor kun den ene fulgte den andre (svak relasjon). Dette ble utgangspunktet for et regneark og en nettverksgraf, laget med programmet Gephi, med personer det ville være relevant å undersøke nærmere. (Se vedlegg, figur 3.)

Analysen av omgangskretsen til Kris avdekket en ny person, «Ken». Ken ble fort interessant for oss, fordi vi fant et bilde på hans Instagram-profil som var identisk med et bilde publisert av x66 på Telegram. Vi hadde lært i andre saker at cyberkriminelle ofte deler tilgang til en konto. Vi fikk nå en ny hypotese: At Kris og Ken samarbeidet om svindler-identiteten x66.

For å undersøke dette nærmere, lagret vi alle Kens innlegg også. Da vi gikk gjennom dem, la vi merke til et bilde hvor han poserte slik at en tatovering var synlig på venstre underarm. Tatoveringen dro vi kjensel på. Vi hadde sett den tidligere – i en video som x66 hadde publisert Telegram. Videoen viste en mann bakfra, med hendene bak ryggen, hvor tatoveringen var synlig på venstre underarm. For å være helt sikre på at det var den samme tatoveringen, la vi bildene oppå hverandre. Det var full klaff. (Se vedlegg, bilder 4). Altså var det sannsynlig at Ken hadde en tilknytning til x66.

## **6.6 Bruk av KI-assistent og råd fra gullsmed**

NRK har en bedriftsavtale med OpenAI om bruk av samtaleassistenten ChatGPT. Dette KI-verktøyet, som lå bak NRKs brannmur, var nyttig i prosjektet på flere måter. Det ble blant annet brukt til å foreslå hvilke klær, smykker, og armbånd vi observerte i bilder postet av Kris, Ken og x66. Vi brukte forslagene som utgangspunkt for å lete på luksusmerkene egne nettsider. Slik fikk vi verifisert merkene, produktene og hva de kostet.

Vi dro på besøk til en gullsmedforhandler i Oslo for å lære mer om smykker i denne prisklassen. Vi fikk gode innspill om forfalsking, noe som gjorde at vi la inn forbehold i saken vi publiserte, av typen «dersom ringen er ekte, koster den...». Dette var viktig, siden vi ikke selv kunne fastslå om smykkene svindlerne poserte med var ekte.

## **6.7 Stedsverifisering av bilder**

Når vi nå visste at Kris, Ken eller begge to sto bak kontoen til x66, måtte vi forsøke å finne dem og konfrontere dem om deres svindelvirksomhet.

I enkelte innlegg på TikTok og Instagram hadde de selv tagget lokasjoner i Bangkok. I tillegg brukte vi spor i bildene, som logoer, landemerker eller skilt, for å plassere bildene geografisk. Vi brukte blant annet omvendt bildesøk, Google Earth, og KI-assistenter for å fastslå hvor og når bilder og videoer ble tatt. Slik identifiserte vi et gatekryss i Xi'an i Kina og en rekke steder i Bangkok.

I tilfellene der vi kunne fastslå en lokasjon, la vi inn koordinatene på et kart. Slik kunne vi visuelt se hvilke steder som gikk igjen. De viste blant annet at x66, Kris, og Ken ofte hadde publisert innhold fra en spesifikk bydel i Bangkok. Opplysningene fra stedsverifiseringen var sentrale i planleggingen av vår reportasjereise til Bangkok. Stedsverifiseringen gjorde at vi kunne diskutere oss frem til en prioriteringsliste over steder vi ville oppsøke, for å finne Kris og Ken i den fysiske verden.

## 7. Infiltrasjon

### 7.1 Svindelkurs og etiske rammer

Mens vi jobbet med å forberede reisen til Bangkok og styrke dokumentasjonen på koblingen mellom x66 på Telegram og Kris på Instagram, ville vi følge et tredje spor: Vi hadde nemlig sett at x66 skrev på Telegram om svindellæringer. Kunne vi også bli lærling hans? Det spurte vi x66 om, gjennom den falske Telegram-brukeren vi tidligere hadde brukt til å kjøpe Magic Cat-lisens fra ham. X66 bekreftet at han kunne tilby oss nettkurs mot betaling.

Å delta på svindelkurs ville være en ukonvensjonell metode, som krevde redaktørvurdering. Vi fikk grønt lys til å delta, men med tydelige kjøreregler: Det var lov å lyve om hvem vi var og hvorfor vi ville ta kurset. Det var derimot ikke lov å initiere eller medvirke til svindel, som å sende ut lure-meldinger. Dessuten måtte vi, før vi avbrøt kurset, fortelle at vi egentlig var journalister og konfrontere x66 med våre funn. Vi utdyper de etiske vurderingene i kapittel 14.

### 7.2 Forberedelser og teknisk oppsett

Vi rigget til et kontor i et kjellerrom hos NRK, med en datamaskin kun til kurs-deltakelse. Datamaskinen ble reinstallert med nytt operativsystem og satt opp kun for dette formålet. Den var utstyrt med et Debian operativsystem (Linux) og OBS opptaksoftware, slik at vi fikk lagret alt som skjedde. VPN innstilt på Singapore tok oss ut på internett slik at IP-adressen ikke kunne spores tilbake til NRK eller Norge. I tillegg hadde vi en Android-telefon, uten simkort, med samme VPN-oppsett, for å kunne kommunisere med x66 resten av døgnet – om nødvendig. Telefonen hadde et vilkårlig telefonnummer fra tjenesten Hushed.

For å fremstå som en troverdig svindler måtte vi ha en plausibel bakgrunnshistorie. Vi konstruerte en fortelling om at vi kom fra Latvia, hadde middels resultater fra andre typer bedrageri og ville bli bedre på meldingssvindel. X66 kjøpte historien og tok oss inn som svindelspire. I mars 2025 var vi i gang.

### 7.3 Mobilinnsamling og uthaling av tid

I starten sendte x66 korte og poengterte meldinger om hvordan vi skulle skaffe mobiler og sette dem opp, slik at de var klare til masseutsendelse av lure-meldinger. I stedet for å kjøpe nye mobiler, lånte vi gamle NRK-firmatelefoner som for tiden var uten eiere – både iPhone og Android – og tok bilder av disse. Da var x66 fornøyd og ga nye instruksjoner.

De etiske kjørereglene gjorde at vår taktikk ble å hale ut tiden, ved å fremstå som nybegynnere og stille mange spørsmål. Slik samlet vi mest mulig informasjon. Etter hvert som tiden gikk ble x66 mer pratsom. Han oppga detaljer om sin kriminelle virksomhet og svindlernes modus, som vi kunne sjekke med andre kilder. Han skrøt

av hvor mye han hadde tjent på svindel (opptil 100 000 kroner på én dag). Hvis summen var korrekt, kunne det forklare bildene hans fra luksuriøse shoppingturer og reiser. Vi var veldig spente på hva som kom, og hvor langt vi ville komme i kurset, før vi måtte avbryte. Dialogen varte i fire uker, og vi brukte opplysninger derfra i flere av sakene våre.

#### **7.4 Bankkort-testing og svenske banker**

Underveis kom x66 med en oppsiktsvekkende påstand. Han hevdet at svindlerne foretrakk norske bankkort fremfor svenske, fordi de norske kortene var enklere å knytte til en digital lommebok. Som bevis sendte han oss et bilde av et nylig stjålet bankkort fra en uheldig DNB-kunde. Påstanden om at svindlerne foretrakk norske kort fremfor svenske, ville vi undersøke.

Fra kolleger samlet vi bankkort fra ti norske banker til en test. Så brukte vi samme metode som svindlerne: Vi forsøkte å opprette et digitalt kort i en annen persons navn på vår egen mobiltelefon. Åtte av de ti bankene vi testet, tillot aktiveringskode via SMS som sikkerhetstiltak.

Deretter kontaktet vi de største bankene i Sverige og forhørte oss om hvilke alternativer deres kunder hadde for å aktivere kort i en digital lommebok. Bankene vi snakket med brukte ikke SMS, slik som i Norge. I stedet måtte kundene identifisere seg via en svensk løsning tilsvarende BankID, eller ringe banken. Det så ut som x66s inngående kjennskap til norsk bankpraksis stemte. En sikkerhetsekspert kritiserte norske banker for å sende koder via sms.

#### **7.5 Gamingmetoden**

En dag beklaget x66 sent svar på et teknisk spørsmål, ved å dele et bilde fra dataspillet Counter-Strike (CS). Kunne vi bruke spillet til å forsterke relasjonen vår, og finne flere spor til hans virkelige identitet? Vi bestemte oss for å prøve.

Noen dager senere sendte vi et bilde fra CS tilbake til x66, uten videre forklaring. Han responderte raskt og spurte om vi også gamet. De neste dagene ble dialogen med x66 ispedd bilder og referanser fra CS. Vi foreslo å spille sammen, og rigget til et hjemmekontor med opptaksutstyr for det formålet. Vi lagde også en falsk profil på CS, som ikke kunne spores til NRK. Av ulike årsaker ble det ikke noe spilling, men dialogen om CS ga oss likevel verdifull informasjon. Når man spiller CS ligger bitte små versjoner av profilbildene til alle deltakerne øverst i skjermen. I et bilde som x66 hadde sendt gjenkjente vi én av profilene: En ung mann sittende på panseret av en gul sportsbil. Dette bildet hadde vi sett før - på profilen til Kris på Instagram. (Se vedlegg, figur 2 – gul ramme) At det samme bildet dukket opp begge steder, var enda en sterk indikasjon på at vi hadde funnet rett mann.

## **7.6 Digitale og fysiske metoder smelter sammen**

Mot slutten av kurset smeltet de digitale og fysiske metodene våre sammen. Vi chattet med x66 samtidig som vi reiste til Thailand for å lete etter ham. Vår hypotese var at direkte digital dialog med x66 på kurset, samtidig som vi jaktet på ham i den fysiske verden, ville øke sannsynligheten for å finne ham. En journalist fra tyske BR, som vi samarbeidet med, deltok også på turen til Bangkok.

## **8. Reportasjereise til Bangkok**

### **8.1 Fra butikkdør til butikkdør**

På Telegram hadde x66 delt kvitteringer fra handleturer til luksusbutikker, der deler av adressene og andre detaljer var synlig. Søk på butikknavn, adresser, og andre detaljer gjorde at vi identifiserte flere fysiske butikker som stemte overens med kvitteringene. Da vi kom til Bangkok dro vi innom flere av dem. Der fremla vi kvitteringsbildene for ansatte. I flere butikker fikk vi bekreftet at kvitteringene så ekte ut, men de ville ikke dele informasjon om kunder.

### **8.2 Telegram-bot**

Våre tyske samarbeidspartnere hjalp oss å bygge et lite dataprogram som varslet vår Telegram-bruker om nye «stories» og innlegg på Instagram-profilene til Kris, Ken og kretsen rundt dem. Slik oppdaget vi at en kvinne i kretsen rundt Kris var på en loungebar. Siden vi var på plass i Bangkok, kunne vi sjekke opplysningene teknologien ga. Vi dro dit og så at hun var der. Vi fulgte med i flere timer for å se om x66 ville dukke opp. Det gjorde han ikke. Da kvinnen dro av gårde i en drosje, fulgte vi etter i en annen drosje. Kanskje hun skulle til leiligheten til Kris? Dessverre mistet vi henne i trafikken.

### **8.3 Fra bardisk til bardisk**

Vi besøkte flere utesteder som vi visste var hyppig besøkt av Ken. På et av dem kjente vi igjen en ansatt som hadde blitt avbildet av Ken i sosiale medier. Vi viste mannen bildet og han sa uoppfordret: «Det er Ken.» Senere kom den ansatte løpende etter oss og sa at Ken ville snakke med oss. Vi opprettet kontakt med Ken på meldingsappen Line. Dette var et gjennombrudd.

### **8.4 Konfrontasjon med Ken og Kris**

Ken sendte NRK en melding på meldingsappen Line. Det ble starten på et døgn med meldinger frem og tilbake. Han ville vite hvorfor vi lette etter ham. Vi ville møte ham. Kompromisset ble en telefonsamtale mens vi var i Bangkok. Dette var vår første mulighet til å fremlegge for Ken dokumentasjonen som koblet ham til x66 og kortsvindel.

Vi ringte fra hotellrommet og gjorde videoopptak av samtalen. Han hevdet å være en forretningsmann, men nektet å fremlegge dokumentasjon på dette. Kort tid etter samtalen sendte han oss et spesielt bilde. Det viste en hånd som holdt en pistol og en rekke andre skytevåpen. (Se vedlegg, bilde 3). I tillegg skrev han at vi måtte komme på besøk, så han kunne banke oss opp. Deretter slettet Kris flere bilder på Instagram og endret brukernavnet på plattformen. Vi besluttet ikke å gjøre flere forsøk på fysiske møter i Bangkok med personene vi undersøkte.

Like før vi reiste tilbake til Norge ringte vi det thailandske nummeret vi hadde funnet på videoen til x66 på Telegram, altså nummeret som hadde ledet oss til Kris. Men vi fikk ikke noe svar, så vi sendte en melding. Vi skrev at vi var journalister og delte våre viktigste funn om svindelaktiviteten. Den vi snakket med, nektet for enhver kjennskap til svindel.

## **8.5 Konfrontasjon med x66**

For å være sikker på at x66 hadde fått muligheten til samtidig imøtegåelse, valgte vi å benytte vår direkte kanal via svindelkurset. Vi kastet masken og sa at vi ikke var en svindellærling, men en gruppe journalister. Deretter konfronterte vi ham med våre funn og ba om imøtegåelse. Han nektet for å være Kris eller Ken, men svarte forbausende nok på mange spørsmål. Like etterpå slettet han chatmeldingene fra opplæringen. Det gjorde ikke noe. Vi hadde naturligvis kopiert dem løpende.

Like etter at vi hadde avslørt hvem vi var, ble Instagram-kontoen til Kris slettet. At dette skjedde samtidig, måtte bety at x66 hadde kontroll over Kris' Instagram-konto, eller at x66 hadde direkte kommunikasjon med noen som hadde det. Dette understreket for oss at vi hadde funnet riktig person.

## **9. Jakten på Darcula**

### **9.1 Dialog med eksperter**

I jakten på den mystiske skikkelsen Darcula, hadde ekspertene i Mnemonic gjort noen innledende undersøkelser. Disse fikk vi innsyn i og ettergikk. NRK og Mnemonic jobbet deretter parallelt i en lengre periode med å gjøre nye funn og kvalitetssikre dem. Vi delte substansielle funn med hverandre, for å kunne drøfte og sammenligne dem. Dette var viktig for at flere brikker skulle falle på plass.

### **9.2 Metadata fra Telegram**

Det fantes veldig få bilder og innlegg fra Darcula på Telegram. Han skrev mest om programmet Magic Cat, og ga tekniske løsninger til de andre svindlerne. De 40.000 chattene vi leste gjennom inneholdt ingen identifiserende opplysninger om Darcula. Det første store gjennombruddet kom ved å analysere metadataene i fire bruksanvisninger han hadde delt. De handlet om hvordan installere Magic Cat.

De fleste sosiale medier sletter normalt informasjon om hvem som opprettet og sist redigerte en fil, men det gjør ikke Telegram. Det er flere måter å hente ut metadata fra mange filer på, men en av de enklere metodene er å benytte gratisprogrammet ExifTool med denne terminal-kommandoen: `exiftool . -csv > metadata_export.csv`, når man befinner seg i mappen med filene. Slik kunne NRK se at bruksanvisningenes metadata inneholdt en variant av Darculas juridiske navn: Yucheng C.

### **9.3 Søk på digitale identifikatorer**

Vi brukte verktøy som Osint Industries for å undersøke om en e-postadresse, et brukernavn eller et telefonnummer var knyttet til en digital tjeneste, som for eksempel PayPal. Slike verktøy kan i mange tilfeller også vise andre telefonnumre, e-postadresser og brukernavn.

Slike søk på Darcula ga treff på et stort antall personlige digitale identiteter, men med strenge personverninnstillinger. Nøkkelen til å avdekke identiteten hans var derfor å sy sammen funn fra mange steder. Flere digitale tjenester oppga ulike bruddstykker av et kinesisk telefonnummer. Bruddstykkene var verdifulle brikker i puslespillet som til slutt førte til et komplett telefonnummer.

### **9.4. Flytdiagram til å strukturere og vekte funn**

Til sammen kartla vi over 50 digitale identiteter som hadde tilknytning til Darcula. Vi samlet sentrale funn i et flytdiagram laget i gratisprogrammet draw.io. En forenklet variant av skjemaet (se vedlegg, figur 4), viser hvordan funnene knytter det kriminelle aliaset Darcula til personen Yucheng C. Dette var viktig for oss for å sikre at vi hadde flere uavhengige spor og kilder som ledet til den samme personen. Oversikten gjorde også redaktørens jobb enklere når de skulle vurdere grad av identifisering i saken.

### **9.5 Slik fikk vi et kinesisk ID-kort**

Med det kinesiske telefonnummeret kunne vi få hjelp av en kilde som har Kina som spesialområde. Kilden fikk bekreftet at Yucheng C. var eier av telefonnummeret. Telefonnummeret var også viktig for å få tak i identitetskortet til Yucheng C. Vi så nærmere på ID-nummeret på kortet. De første seks sifrene viste regionen eller området hvor en person ble født. Slik lærte vi noe nytt om Yucheng C. Han var født i Henan-provinsen.

### **9.6 Samtidig imøtegåelse med Darcula**

Etter å ha jaktet på Darcula i rundt ett år var det omsider tid for å ta direkte kontakt. I vår første henvendelse brukte vi hans virkelige fornavn, for å vise at vi visste hvem

han var og for å få hans oppmerksomhet. «Yucheng, jeg ønsker å snakke med deg», skrev vi på Telegram.

Senere samme dag sendte vi over mer informasjon om hva vi planla å publisere. Vi fikk ikke svar på meldingene. Dagen etter sendte vi en utfyllende redegjørelse til tre e-postkontoer tilknyttet Darcula. Vi ringte samtidig to telefonnumre koblet til Darcula, uten å komme gjennom.

Endelig sendte vi en ny runde med e-poster og la igjen en offentlig kommentar på en personlig konto tilknyttet Darcula. I kommentaren fortalte vi kort hvem vi var, at vi arbeidet med en sak om Magic Cat og viste til tidligere e-poster fra oss.

Samme dag ble vi kontaktet på WhatsApp av en person som hevdet å ha fått en av e-postene vi hadde sendt til Darcula. Personen identifiserte seg ikke med fullt navn, men hevdet han hadde jobbet med Yucheng. Vi ba om dokumentasjon på påstandene hans, uten å få det. Vi holdt dialogen gående i flere dager, uten at det kom nye svar på våre spørsmål eller nyttige opplysninger.

Da vi publiserte hadde ikke Darcula vært aktiv på Telegram siden vi sendte vår første melding. Det var høyst uvanlig. Tidligere hadde han vært aktiv på Telegram svært ofte. Etter publisering ble brukeren hans på Telegram og andre steder slettet.

## **10. Kinesiske hvitvaskere i Norge**

Etter første publisering fikk vi høre at politiet etterforsket en sak med mulige koblinger til Magic Cat. En kinesisk statsborger var pågrepet i Norge, siktet for hvitvasking av stjalne kort. Nå så vi en mulighet til å finne ut hva som skjedde i Norge med kortene som svindlerne fisket inn. På Telegram hadde vi lest om metoder for hvitvasking, men visste ikke at kinesiske svindlere gjorde det i Norge.

Politiadvokaten på saken fortalte at tiltalen var tatt ut og saken berammet. Vi dro for å overvære hovedforhandlingen. Etter at dommen falt, ba vi politiet om innsyn i dokumenter og kopi av overvåkningsvideoene presentert i retten. Vi antok at det ville være vanskelig å avslå innsyn i materiale som var lagt frem i åpen rett. Vi viste til Riksadvokatens veileder til innsyn i straffesaksdokumenter, og argumenterte for at saken hadde stor samfunnsmessig relevans fordi befolkningen stadig utsettes for svindelforsøk.

Innsyn ble innvilget. Dokumentene var viktige for at vi selv kunne forstå og dernest fortelle publikum om hvitvaskingsmodus. Etterforskningen konkluderte ikke om hvordan kortdetaljene var fisket inn.

## **11. Historiefortelling**

Vi besluttet å dele opp hovedsaken i to deler, fordi det ville være for komplisert å skrive om jakten på både x66 og Darcula i én og samme sak. Funn, scener,

avsløringer og cliffhangers ble skjematiskert, som hjelp til skriveprosessen. For at saken ikke kun skulle appellere til et teknisk kompetent publikum, måtte vi forenkle begreper, men samtidig sikre at informasjonen var korrekt.

Vi bestemte oss for å publisere hovedsakene og en av nyhetsoppfølgerne på engelsk, siden svindelmeldinger er et globalt problem. Dessuten hadde mange internasjonale nettsteder tidligere omtalt Darcula. Nå kunne vi fortelle hvem det faktisk var.

## **12. Spesielle erfaringer**

Da vi viste frem Magic Cat for sikkerhetsekspertene og digitaliseringsminister Karianne Tung skjønnte vi hvor virkningsfullt det var å kunne demonstrere det svindlerne faktisk gjorde og ikke bare fortelle om det. Vi bestemte oss for å skru programmet fra hverandre og sette det sammen igjen, for virkelig å forstå det.

Mnemonic hadde funnet en måte å lure programvaren til å tro at den hadde en gyldig lisens. Slik fungerte det uten å være knyttet til en kriminell server. Den trygge versjonen av Magic Cat kunne vi kjøre på en egen dedikert maskin.

Etter publisering av hovedsakene fikk vi en rekke invitasjoner til å holde foredrag. Her brukte vi vår egen versjon av Magic Cat for å demonstrere programmet. Svindlekspertene, politi og bankfolk har for første gang fått se hvordan svindelen faktisk skjer, at det foregår i sanntid og hvordan det er mulig å svindle folk i så stor skala. Vi tror denne kompetansehevingen kan bidra til å forebygge og stanse svindel fremover.

## **13. Motstand**

Det har vært krevende å finne identifiserende opplysninger om svindlerne, fordi de er tekniske kompetente og har gått langt for å skjule sine spor. Vårt to måneder lange blindspor og undersøkelser i Canada er et godt eksempel på det. I perioder var vi veldig usikre på om vi ville komme i mål med å identifisere og konfrontere x66 og Darcula.

## **14. Etikk**

### **14.1 Bruk av falsk identitet**

Vi har opptrådt med falsk identitet på svindelkurs. Vår vurdering var at det ikke ville være mulig å delta på kurset hvis x66 visste at vi var journalister. Kurset var en unik mulighet til å finne opplysninger om x66s person, hva han driver med som svindler, finne spor etter oppholdssteder, og lete opp informasjon som kunne underbygge eller korrigere våre foreløpige opplysninger om hvem han var.

Vi har også opptrådt med falsk identitet i svindelgrupper på Telegram. Som i resten av prosjektet var grunnregelen at vi ikke skulle delta i kriminell aktivitet, eller påskynde andre til å gjøre noe ulovlig. I disse gruppene var vi uansett i hovedsak observatører.

NRK mener bruken av falsk identitet har vært forsvarlig fordi det har skaffet oss unik informasjon om hvordan svindlerne jobber, også opp mot Norge. Det har vært åpenbart at informasjonen ikke kunne fremskaffes med åpen identitet som journalister.

## **14.2 Betaling til svindlerne**

I dette prosjektet har NRK betalt rundt 1400 kroner for en lisens til Magic Cat i én uke, samt rundt 13.000 kroner for å delta på svindelkurs. Etter en etisk diskusjon med redaktør kom vi frem til at pengebruken kunne forsvares fordi pengesommene utgjorde en svært liten del av et omfattende svindel-økosystem med store penger i omløp. Betalingen fra NRK var altså ikke viktig for svindelens eksistensgrunnlag eller skala. Den var derimot helt nødvendig for å fremskaffe noe av den mest sentrale dokumentasjonen i saken.

## **14.3 Identifisering av svindlerne**

NRK har publisert bilde av ansiktene til x66 og Darcula, i tillegg til fornavn og første bokstav i etternavnet hans: Yucheng C. Vi har også publisert en sladdet versjon av hans ID-kort, hvor ansiktet var godt synlig.

Flere andre hadde forsøkt, før oss, å finne ut hvem Darcula kunne være. Vi måtte dokumentere at vi hadde lyktes. Samtidig vurderte vi at det ikke var dokumentarisk nødvendig å bruke fullt navn, fordi han og x66 er fra en annen verdensdel og ikke bruker sine ekte navn i svindelen. Å publisere navnene deres ville altså ikke hjelpet folk til å finne ut om de var blitt svindlet.

## **15. Dette er nytt**

- NRK har avslørt Magic Cat – et av de mest populære dataprogrammene for meldingssvindel verden over.
- Vi har avslørt omfanget av meldingssvindel fra Magic Cat i en syv måneders periode, både i Norge og globalt, samt publisert tall fra hvert enkelt land. Vi avdekket også at Magic Cat ikke tilbyr falske nettsider på kinesisk.
- NRK har avslørt identiteten til personen bak programmet: Yucheng C.

- NRK har avslørt storsvindleren x66, og fortalt hvordan han gir opplæring til nye svindlere.
- Vi har vist hvordan meldingssvindel fungerer steg-for-steg.
- Vi har avslørt at svindlere foretrekker norske bankkort, fremfor svenske, fordi mange norske banker benytter verifisering via tekstmelding for å legge bankkort til digitale lommebøker.
- Vi har fortalt hvordan kinesiske hvitvaskere opererer ved å tappe stjålne bankkort gjennom å handle gavekort på dagligvarebutikker i Norge.
- Vi har dokumentert hvordan dagens lovverk vanskeliggjør kampen mot digitale bedragerier ved at banker ikke har lov til å dele informasjon ved mistanke om svindel.

## 16. Konsekvenser

- Etter at NRK konfronterte Yucheng C. og snakket med personen som hevdet å ha jobbet med ham, stengte svindelprogrammet Magic Cat ned i en periode. Dermed kunne svindlere ikke lenger bruke det til å lure hundretusener av mennesker over hele verden, slik de hadde gjort uforstyrret siden 2023.
- Etter at NRK konfronterte Darcula, sluttet han å logge seg på Telegram. Kort tid etterpå slettet han sin bruker.
- Etter at NRK viste digitaliseringsminister Karianne Tung hvordan Magic Cat fungerte, ba hun umiddelbart en ekspertgruppe hos Nasjonal Kommunikasjonsmyndighet (Nkom) undersøke tiltak mot meldingssvindel.
- Nkom har sammen med Økokrim, i styringsgruppen til ekspertgruppen mot svindel, vedtatt å forlenge og utvidet mandatet for ekspertgruppen til å gjelde også internettbaserte tjenester og meldingstjenester.
- Nkom inviterte Google til et møte med den nasjonale ekspertgruppen mot digital svindel, med henvisning til NRKs saker.
- Etter å ha lest NRKs saker, valgte Posten Norge å levere til politiet en samlet anmeldelse av 347 tilfeller av svindelforsøk. Saken ble henlagt i desember.
- Flere banker og selskaper oppgir å ha endret sine sikkerhetsrutiner etter at NRKs saker ble publisert, uten at de ønsker å dele detaljer om endringene.

- Etter første publisering har prosjektets journalister holdt totalt 25 foredrag om arbeidsmetoder og funn, på forespørsel fra blant annet Riksadvokatens statsadvokatmøte, NAFCoop (Økokrim fra Norge, Sverige, Danmark, Finland og Island), Finans Norge, Nasjonal Sikkerhetsmyndighets partnernetverk, Cybersikkerhetsenteret for forskning og utdanning, Næringslivets sikkerhetskonferanse, Politihøgskolen og UDIs faggruppe for OSINT.
- Google har saksøkt Yucheng C. og 24 andre ikke-navngitte personer gjennom en føderal domstol i New Yorks Southern District i USA. Søksmålet viser syv ganger til NRKs avsløringer som faktagrunnlag. Google har bedt domstolen om en midlertidig forføyning mot Darculus infrastruktur på nett, noe som vil gi dem juridisk rett til å ta kontroll over infrastrukturen og stenge den ned.

# Publiserte saker

## Nett

4. mai 2025: [På innsiden av svindelsentralen](#)

4. mai 2025: [Jakten på Darcula](#)

8. mai 2025: [Svindler til NRK: «Du ble nesten en av oss»](#)

13. mai 2025: [Svindlernes bakmann har gått under jorden](#)

28. mai 2025: [Posten blir misbrukt av svindelnettverk - ber politiet ta grep](#)

13. august 2025: [Storsvindlar føretrekker norske bankkort fremfor svenske](#)

19. august 2025: [Posten åtvarar mot ny svindelstorm](#)

6. september 2025: [Tatt på fersken: Kinesere på svindelturné i Norge](#)

9. oktober 2025: [Krev lovendring: Bankane har ikkje lov til å ringe politiet når dei mistenker svindel](#)

17. desember 2025: [Google saksøker svindelnettverk avslørt av NRK](#)

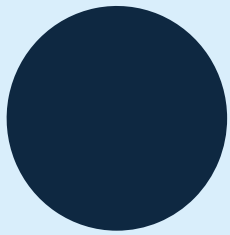
22. desember 2025: [Henlegger svindelanmeldelser fra Posten](#)

## TV og radio

4. mai 2025: [Avslører svindelmetode \(Dagsrevyen\)](#)

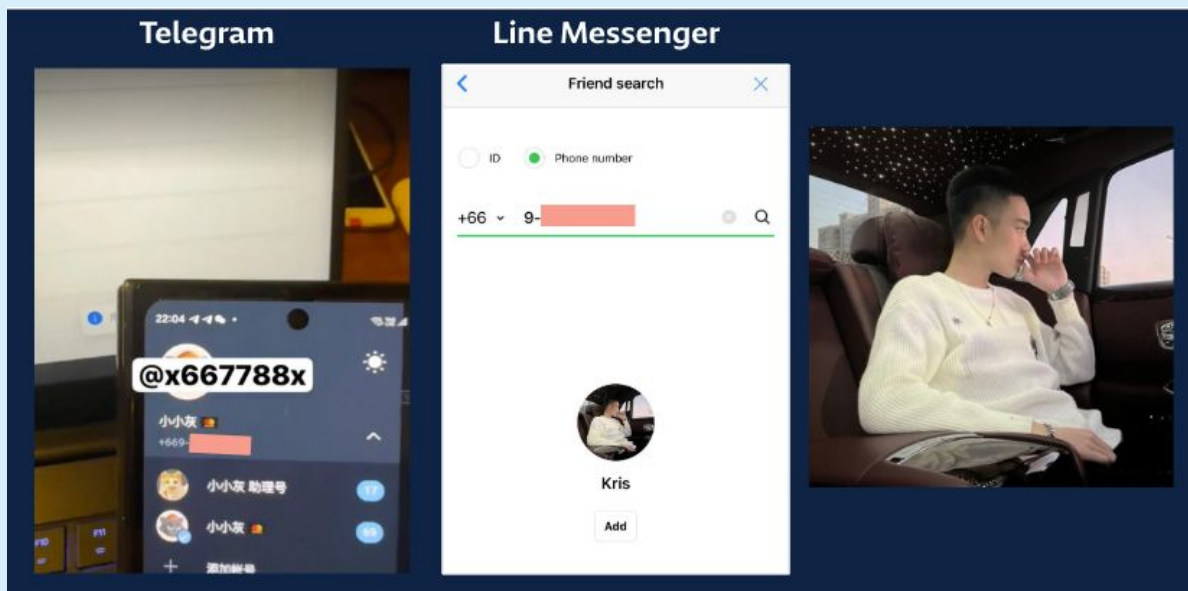
4. mai 2025: Digitaliseringsminister Karianne Tung om [Magic Cat \(Dagrevyen 21\)](#)

9. mai 2025: Levde luksusliv: Avslørt av svindel-jegere (Podkast: Oppdatert)

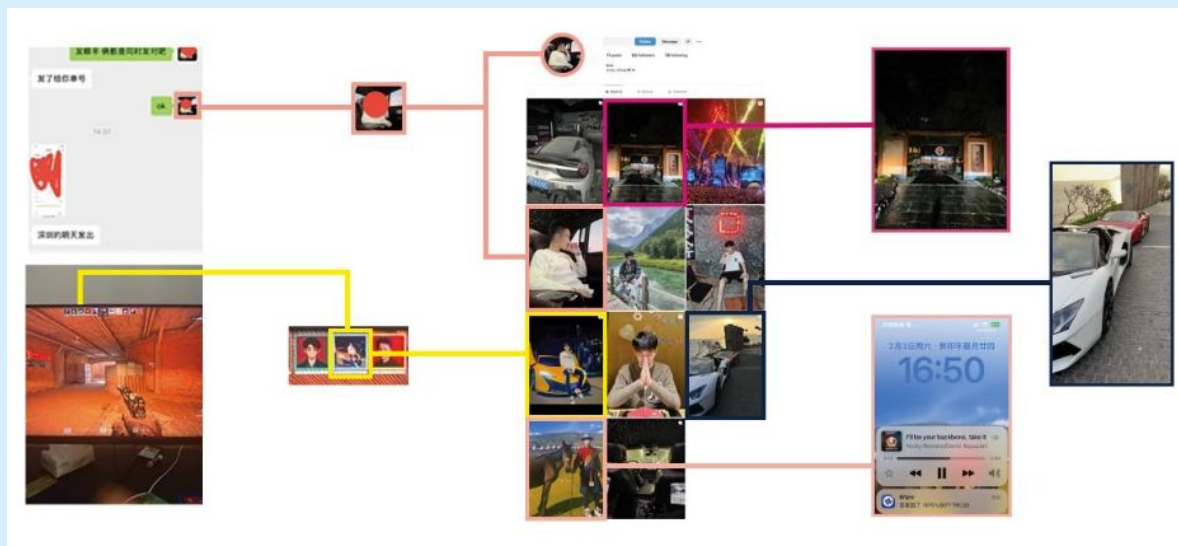


# Vedlegg

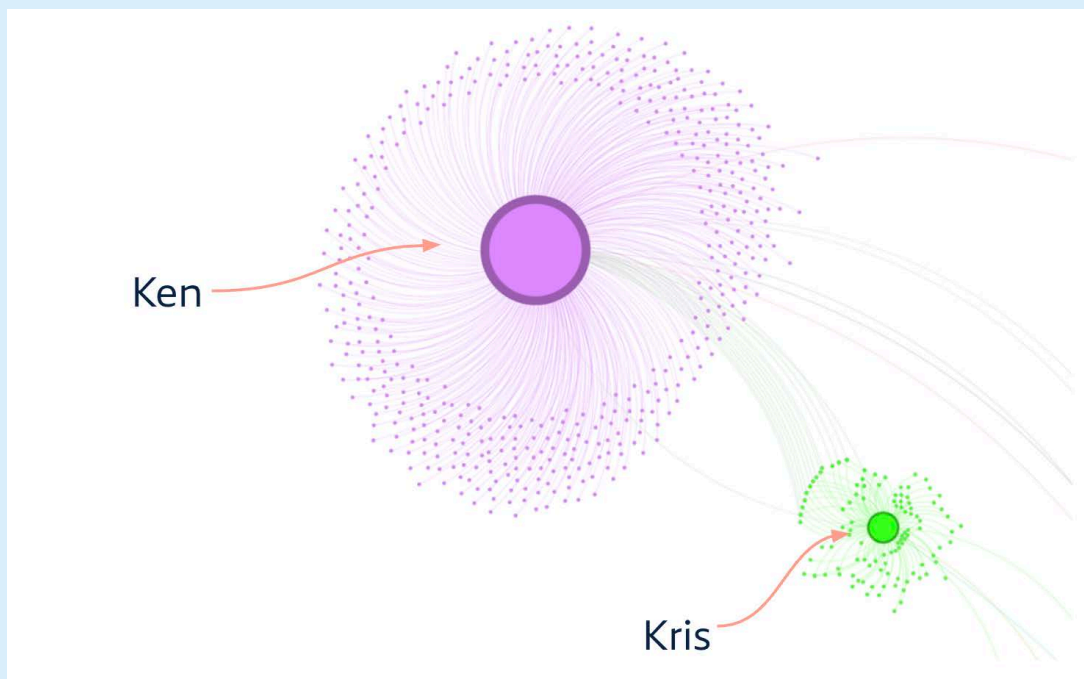
**FIGUR 1:** I en video på Telegram eksponerte brukeren x66 et thailandsk telefonnummer, som var knyttet til en bruker på den digitale tjenesten Line Messenger. Vi fikk profilbildet i høyere oppløsning ved å sende en venneforespørsel.



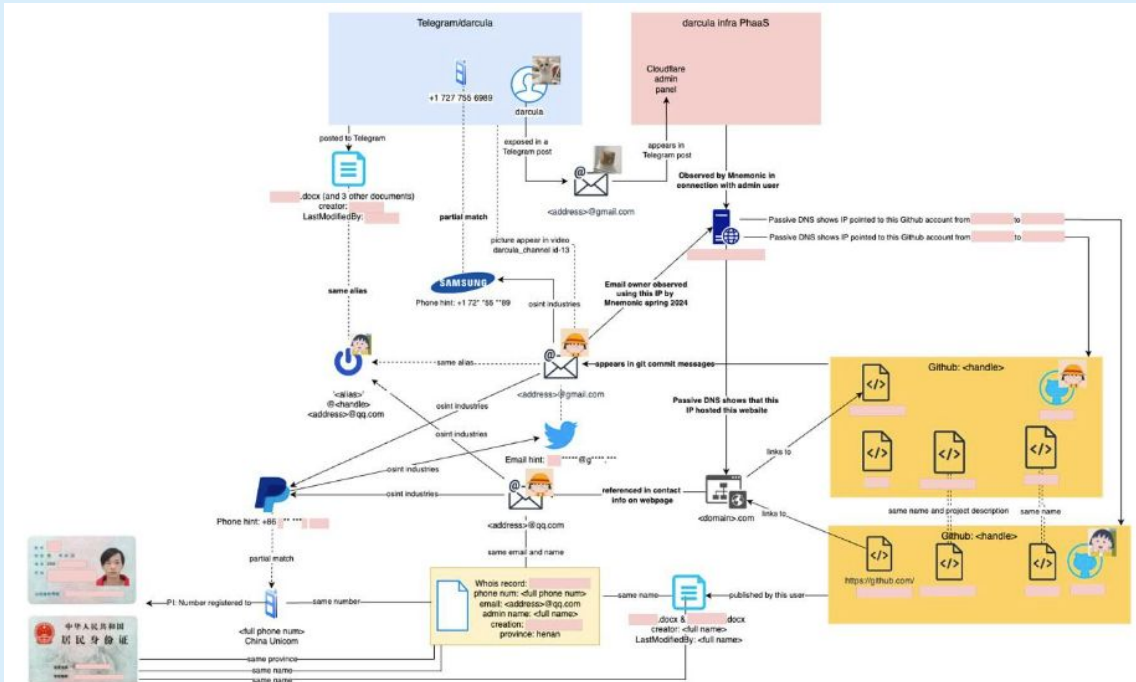
**FIGUR 2:** Koblinger vi fant mellom bilder publisert av svindleren x66 og bilder på «Kris» sin personlige Instagram-profil (midten).



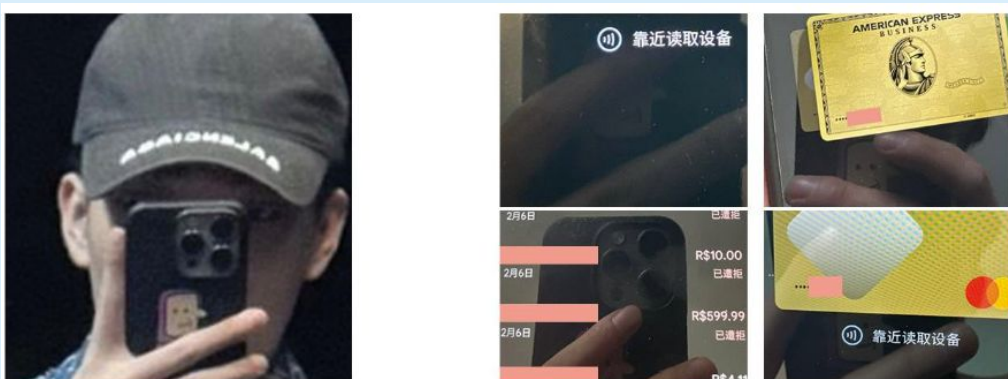
**FIGUR 3:** Et utsnitt av nettverksgrafene laget med programmet Gephi. Trådene illustrerer koblinger mellom Ken og Kris på Instagram



**FIGUR 4:** Flytdiagram, laget i gratisprogrammet draw.io, viser viktige koblinger mellom det kriminelle aliaset Darcula, ulike digitale identiteter og Yucheng C.



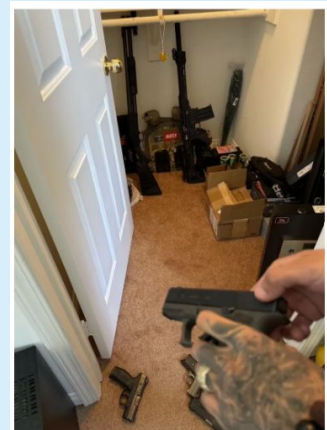
**BILDER 1:** Et innlegg publisert på TikTok (t.v.) viser en mobiltelefon som på baksiden har et karakteristisk klistremerke, av et firkantet hvit smiley-lignende ansikt. Det samme klistremerket er synlig i flere innlegg fra x66 på Telegram (t.h.).



**BILDER 2:** Den samme eksklusive Louis Vuitton-jakken er synlig bak datamaskinen i en post fra x66 på Telegram (t.v.) og i et innlegg på TikTok (t.h.).



**BILDE 3:** Etter at vi konfronterte Ken over telefon i Bangkok, fikk vi tilsendt dette bildet, samt en tekst hvor han truet med å banke oss opp.



**BILDER 4:** Ken la ut bildet til venstre på sin Instagram-konto. Her var tatoveringen på venstre underarm synlig. Bildet til høyre er hentet fra en video x66 delte på Telegram. Vi la tatoveringene oppå hverandre og så da at de var identiske.

