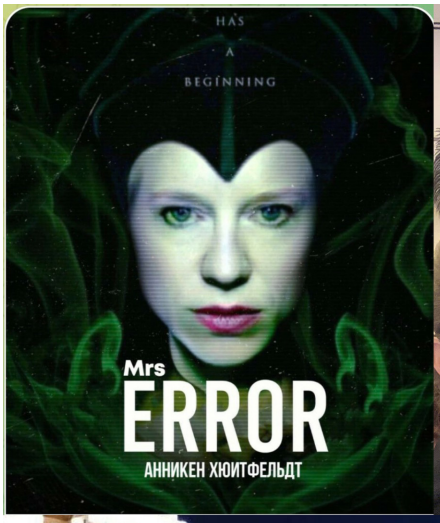
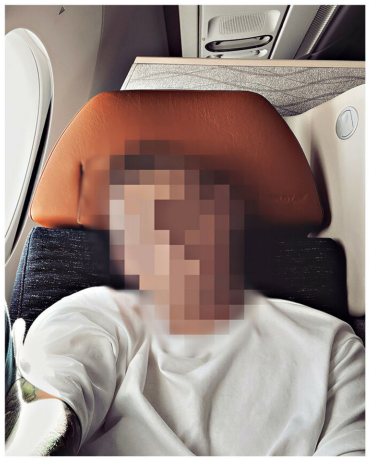
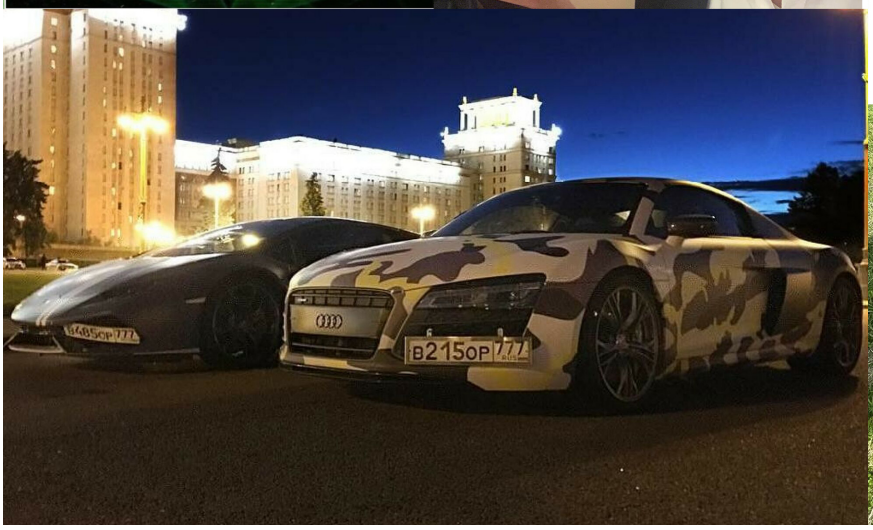
Sporene til Russland







Metoderapport Data-SKUP 2022

Dagbladet

Torgeir P. Krokfjord (Dagbladet) - Thomas Frigård (Kommunal rapport)

Oslo, 14. august 2023

Kontaktadresse: Torgeir P. Krokfjord, Dagbladet, tpk@db.no, tlf 47 41 49 69

INNHOLD

1 Innledning

1.1 Dagbladet har avslørt

- At den russiske hackergruppa Killnet angrep norske myndigheter og medier, og samtidig kom med grove trusler mot Jens Stoltenberg og hans familie
- At den russiske hackergruppa Killnet har sendt penger gjennom kryptobørsen Bitfinex på De britiske jomfruøyer. Ukrainas regjering mener dette er hvitvasking av penger.
- At bitcoin fra omfattende nettsvindel i Norge og andre europeiske land også er sluset til kryptobørsen Bitfinex – der pengene kan vaskes og tas ut i ordinær valuta.
- At det har vært minst 49 hackerangrep mot norske bedrifter de to siste årene, og at hackergrupper fra Russland står bak nesten sju av ti av dem.
- Identiteten til et tosifret antall medlemmer av de russiske hackergruppene Killnet, Conti og Revil. Vi avslørte at flere av dem hadde bakgrunn fra det russiske forsvaret.
- At en russisk smykkegründer, og en russisk eiendomsmagnat, begge aktivt hjalp til med å finansiere hackergruppa Killnet.
- At et russisk ektepar bosatt på Kypros, der mannen jobbet i et stort finansselskap, bisto Killnet med å skaffe penger. Mannen fikk sparken etter avsløringen.
- At rederiet Vard, som produserer den norske etterretningstjenestens spionskip, ble hacket av en hackergruppe der flere medlemmer har fortid i det russiske forsvaret.
- At russiske hackere brøt seg inn i vannsystemet i Drammen, kort tid etter at hackere ville forgifte en drikkevannskilde i USA. Kommunen satte hendelsene i sammenheng.
- At det aldri har vært vær jamming av GPS-signaler på norske flyplasser enn i 2022. Det til tross for at statsminister Erna Solberg i 2020 sa at problemet var borte.

1.2 Innledning

Etter Russlands invasjon av Ukraina, ønsket vi å undersøke russisk aktivitet i Norge. Flere norske virksomheter var angrepet og presset for penger av såkalte «løsepengehackere». Vi ønsket å finne ut hvem hackerne var – og hvor de fikk penger fra. Samtidig var vi presset på grunn av krigsdekningen.Vi kjente til Thomas Frigård fra før – og han og Kommunal Rapport takket ja til et samarbeid. Prosjektet ble omfattende. Her fokuserer vi på datajobbingen. Vi regnet ikke med å kunne slå hackerne på darkweb og programmering. Men kunne vi avsløre dem med åpne kilder?

2 Metode

2.1 Metode: Det mørke nettet

Hvem er hackernes norske ofre? Vi hadde i bransjeartikler og annen medieomtale kommet over den amerikanske sikkerhetsanalytikeren Brett Callow. Vi tok kontakt med ham om de russiske løsepengehackerne. Han påpekte at korrespondansen mellom offer og hacker gjerne foregår på det mørke nettet, der hackergruppene har hatt egne blogger. Mange av dem var nå offline etter en del arrestasjoner i 2021/2022. Callow ga oss darkweb-adressene til Hive og Lockbit – som fortsatt var aktive. På bloggene fant vi at de hadde publisert informasjon om angrep mot flere norske ofre.

Vi sammenstilte denne informasjonen med data fra Teknisk Ukeblad – som hvert år publiserer en tentativ liste over norske ofre for hackerangrep. Og fra sikkerhetsselskap som DarkTracer og HackNotice, som også publiserer jevnlige lister over hackerangrep – med informasjon hentet fra darkweb. Vi hadde nå en liste med 49 norske ofre. Vi kontaktet samtlige 49, og lista ble til sakene: Da hackerne slo til: - Fikk helt noia og Ante ingenting før angrepet: - Dette skjer ikke.

2.2 Metode: Innsyn

Gjennom innsynsbegjæringer på Einnsyn, hos Luftfartstilsynet, Nasjonal kommunikasjonsmyndighet og Kommune Csirt, jobbet vi videre. Vi avdekket en forbindelse fra et dataangrep i USA til et dataangrep mot Drammen kommune – og at norske flyplasser aldri før hadde blitt utsatt for så hyppige russiske støyangrep, som etter invasjonen av Ukraina: Russiske støyangrep mot Norge: - Farlig.

2.3 Angrepet mot Norge

2.3.1 Metode: Telegram

I researchen kom vi over referanser på Twitter til kanalen «Russian OSINT», på meldingstjenesten Telegram. Telegram er en meldingstjeneste på samme måte som Signal og WhatsApp, men det er også en sosial arena siden det er lett å opprette grupper, chattekanaler og diskusjonsforum der. «Russian OSINT» var en prorussisk kanal som delte metodetips og hackernyheter – spesielt nyheter som gagnet Russland, eller svertet Vesten. Vi oppdaget at Russian OSINT repostet flere innlegg fra den russiske hackergruppa Killnet. Killnet og deres kanaler i sosiale medier skulle bli en viktig arena for innhenting av informasjon. Tidligere hadde gruppa vært en produsent av skadeprogramvare, som ble brukt i tradisjonelle løsepengeangrep. Men etter invasjonen av Ukraina hadde Killnet erklært seg som en del av den «russiske cyberhæren», og blitt en politisk aktør. Killnet opererte flere propagandakanaler på Telegram. De annonserte angrep, postet memes, bilder og video, og hadde over 30 000 følgere.

Killnet publiserte også fortløpende hvem de selv angrep. Og i noen tilfeller annonserte de angrepene sine på forhånd. 22. juni sperret vi opp øynene. I Telegram-innlegget fra Killnet tittet Jens Stoltenbergs blide ansikt mot oss – fra innsiden av et pass. Killnet la ut et bilde av det de påsto var NATO-sjefens pass. Det så ut som et autentisk, norsk identitetsdokument. Om dette ble spredt ville det utgjøre en stor sikkerhetsrisiko for NATO-sjefen. Gruppa kom videre med trusler mot Stoltenberg og familien hans: «Jeg glemte å introdusere deg for vår fiende nummer 1 – Jens Stoltenberg. Denne djevelen vil svare for ethvert liv til en russisk soldat. Og også hans familie, hans barnebarn og hans støttespillere vil svare.» Vi tok skjermdumper av bildet. Planen var å jobbe med en sak om Stoltenberg til publisering etter sommeren. Ei uke seinere, endret den planen radikalt.

Suget i magen

Mens toget til jobb tikket inn på perrongen, om morgenen 29. juni, dukket et manipulert bilde av Anniken Huitfeldt opp på skjermen på mobiltelefonen. I magen kjentes den følelsen som kommer når nyheten du jobber med er av det virkelig store slaget. Når du vet at du, mest sannsynlig, sitter på dagens store sak. Killnet annonserte at de var i ferd med å angripe Norge: på angrepslista de delte på Telegram, sto både NAV, Arbeidstilsynet, politiet, Bank ID og ID-porten, samt medier som VG og NRK. Arbeidstilsynets nettsider var nede.

Vi begynte umiddelbart å ringe rundt. Arbeidstilsynet hadde registrert at nettsidene deres fungerte dårlig eller var tatt ned. De ante imidlertid ikke hva som hadde skjedd, før vi ga dem beskjeden: - Russiske hackere sier de angriper dere – akkurat nå. Selv om Nasjonal Sikkerhetsmyndighet seinere sa at deres folk hadde kjent til angrepet, var ikke kommunikasjonsavdelingen oppdatert da vi ringte.

Som vi kommer tilbake til fikk vi kontakt med en av hackerne. Han hevdet i et intervju med oss at angrepet kom fordi Norge stanset godstransport fra Russland til Barentsburg på Svalbard.

2.3.2 Metode: Folkeregisteret

Angrepet mot Norge aktualiserte Killnets trusler mot Jens Stoltenberg. Det var bare et tidsspørsmål før andre medier fant samme informasjon. I bildet Killnet delte sto Stoltenbergs påståtte

personnummer oppgitt. Vi har tilgang til Folkeregisteret via nettportalen Infotorg, og søkte opp Stoltenberg: Men personnummeret stemte ikke. Det sto oppgitt et annet personnummer i Infotorg, enn det som sto på det påståtte passet som Killnet delte.

Hva betydde egentlig det? Vi googlet, og fikk opp en rekke nettsteder som oppga at det kunne være mulig å endre personnummer, om enkelte ekstremt strenge kriterier var oppfylt. Blant dem var at man har fått vedtak om en fiktiv identitet fra politiet eller at det var fattet vedtak om å endre personnummeret av ditt for å forhindre stalking eller lignende. Begge deler kunne teoretisk sett være riktig i Jens Stoltenbergs tilfelle: Vi visste lite om sikkerhetssituasjonen rundt ham som statsminister og NATO-sjef. NATO kom raskt tilbake med en kommentar: Passet er falskt. Det stemte med det vi hadde funnet i Folkeregisteret. Etter å ha gitt alle muligheten til å kommentere, publiserte vi saken om at Killnet truet NATO-sjefen og hans familie. Siri Wiersen hos nyhetsavdelingen begjærte innsyn i korrespondanse mellom UD og Sysselmesteren på Svalbard – og russiske Trust Arktikugol, om matleveransen Killnet-hackeren hadde henvist til. E-postene viste at det var kontakt mellom Norge og Russland dagen før hackingen: Ukjent e-post før angrepet.

2.4 Hvem er hackerne?

På nett bruker hackergruppene pseudonymer, de kommuniserer på det mørke nettet – gjemt bak VPN-løsninger, kryptert kommunikasjon og lukkede forum. Som nevnt i innledningen til metoderapporten, hadde vi ingen ide om at vi i løpet av noen måneder ville kunne hevde oss mot hackerne på deres egne fagfeltt. Hva kunne vi finne ut om dem, ved å bruke åpne kilder?

2.4.1 Metode: Personsøk i Telegram

Da Killnet annonserte angrepet på Telegram, boblet det av aktivitet inne på kanalen deres. Innleggene om angrep mot Norge fikk raskt tusenvis, av likes og kommentarer.

Vi hadde varsling på telefonen på innlegg i Killnet-kanalen, og hadde derfor lagt merke til det originale innlegget – med sjikanen mot Anniken Huitfeldt og truslene mot Norge – nesten før det hadde fått noen respons fra følgerne. Men en konto gikk umiddelbart i gang med å pushe innlegget, dele det og legge ut forhåndsprodusert PR-materiale. Siden kontoen så ut til å ha forutgående kunnskap om angrepet, ønsket vi å finne ut hvem som sto bak.

Samtidig var Killnet-angrepet en løpende nyhetshendelse der alle de store redaksjonene nå jobbet på høygir. Vi tok kontakt med kontoen – og prøvde samtidig å finne ut hvem det var.

Brukernavnet

Selv om brukeren kan velge å skjule dette i chattegruppene og -trådene sine, har alle Telegram-brukere et kallenavn. Vi klikket oss inn på den interessante Killnet-kontoen, og fant brukernavnet til vedkommende. Mer informasjon sto det ikke der. Vi googlet brukernavnet, og fant flere Some-kontoer med samme brukernavn. Flere av kontoene hadde samme navn og bilder som lignet. Men om kontoene i andre sosiale medier tilhørte samme person, betød ikke det at Telegram-kontoen også var vedkommende. Brukernavnet var ganske generisk, og spilte på en term som er hyppig brukt i datakretser – både blant russisk- og engelskspråklige.

TGscanrobot

Via en russisk kontakt hadde vi blitt tipset om den russiske journalisten Andrei Soshnikov. Han hadde dekket hackergruppene bredt tidligere. Vi tok kontakt med ham, og fra Soshnikov fikk vi tips om å bruke boten TGScanrobot - en automatisert funksjon som, om du sendte den et brukernavn som melding på Telegram og betaler et lite beløp, kunne innhente informasjon om hvilke grupper en spesifikk Telegram-konto er medlem av. Om du har litt flaks, kan bot'en dermed gi ganske mye informasjon både om hva slags interesser en Telegram-bruker har, hvor vedkommende er fra, hva

vedkommende jobber med og så videre. Vi sendte en melding med brukernavnet til den mulige hackeren, til TGScan-boten. Resultatet viste at brukeren vi kommuniserte med på Telegram, var medlem av en rekke grupper som gjaldt både en spesiell by i Russland – og også nærmiljøet i en liten del av denne byen.

Vi bladde igjennom bildene på kontoene vi hadde funnet på andre sosiale medier – på kontoene med samme brukernavn. Der oppdaget vi at denne brukeren hadde geotagget seg selv i nøyaktig det samme, lille nabolaget i en russisk by. Det var nå langt mer sannsynlig at vi hadde funnet riktig mann. Da vi konfronterte mannen med at vi hadde funnet navnet hans, bekreftet han dette. Vi publiserte da et intervju der han sier han deltok i angrepet på Norge.

I samme sak uttaler også en tidligere hacker seg. Det var en mann som tok kontakt – og som selv bisto med informasjon som verifiserte at han trolig snakket sant da han hevdet at han hadde en fortid som medlem i Killnet. Hva dette er kan vi ikke røpe her, av kildevernhensyn. TGScan-roboten ble nyttig også seinere. Seinere på sommeren oppdaget vi at Killnet la ut et innlegg der en aktivist tilknyttet gruppa oppga å være i Oslo. Vedkommende la ut koordinatene til en park på Bekkelaget, og kom med en påstand: Det skulle bli avholdt en «proukrainsk samling» på gressletta. Derfor måtte prorussiske aktivister «mobilisere».

Vi reiste ut den aktuelle kvelden, da Killnet-aktivisten skulle mobilisere, men fant verken russere eller ukrainere. Men på gresset var det imidlertid tagget flere store Z-er – symbolet som indikerer støtte til Russlands invasjon av Ukraina – og teksten: «God morgen, Norge – hilsen Killnet».

2.4.2 Metode: Pimeyes

En av personene som kommenterte på Telegram-innlegget om Bekkelaget, framsto som norsk. Vedkommende var en kvinne, og det var flere bilder av henne på profilen. Vi søkte dem opp i Pimeyes, som er et verktøy for å ansiktsgjenkjenning. Da fikk vi treff på flere sosiale medier-profiler tilhørende en kvinne bosatt i Norge. Vi søkte opp den samme kvinnen med TGScanrobot – altså bot-en på Telegram som vi hadde brukt til å finne en av hackerne i Killnet. Ved å søke opp den norske kvinnens brukernavn på TGScanrobots kanal på Telegram, fant vi ut hva slags grupper og diskusjoner hun hadde deltatt i på Telegram.

Vi gikk så igjennom de andre profilene vi hadde funnet gjennom bildesøk. Informasjonen var sammenfallende, og det var overveiende sannsynlig at vi hadde funnet den norske Killnet-støttespilleren. Vi søkte opp den aktuelle kvinnen i selskapsdatabasen Bizweb, der vi fant hennes fødselsdato, og i Folkeregisteret, som vi har tilgang til via nettportalen Infotorg. Der fant vi ut at hun var opprinnelig russisk, men at hun nå var gift med en nordmann. Vi tok kontakt med henne, og hun stilte etter en lengre vurdering opp til anonymisert intervju.

Bildedumpene

Samtidig som vi gravde i Killnet, etter gruppas angrep mot norske myndigheter, jobbet vi videre med løsepengehackerne som var utgangspunktet for undersøkelsene våre. Spesielt fokuserte vi på Conti, fordi gruppa både har stått bak angrep i Norge og skal ha forbindelser til russisk etterretning.

Fra en kilde som fulgte hackermiljøet tett fikk vi tips om en interessant, anonym Twitter-konto. Den publiserte bilder, navn og informasjon på personer den hevdet var tilknyttet flere av de russiske hackergruppene. Vi tok kontakt med kontoen, men fikk til svar at hen ikke ønsket å snakke med pressen. Publiseringen hadde begynt på vårparten 2022, og fortsatte gjennom sommeren. Vi sjekket kontoen og tok skjermdumper fortløpende – på lekeplasser under utenlandsferie og under dobesøk i middagsselskaper. Vi lagret alle skjermdumper både lokalt på PC og i en tråd på Signal.

To ganger ble kontoen stengt og publiseringen stoppet, men etter en stund var den oppe og gikk igjen, før publiseringen stoppet for godt i midten av juli. Da hadde vi lastet ned informasjon om flere titalls påståtte medlemmer av russiske hackergrupper: Angivelige navn, bilder og personlige detaljer. Materialet som i lekkasjene på Twitter-kontoen stammet eksempelvis fra at hackerne har brukt personlig e-postadresse til å logge inn på forum på det mørke nettet eller på sosiale medier. Det kunne være brukernavn på forum som matcher brukernavn brukt i hacker-øyemed.

Vi kontaktet en rekke kilder i cybersikkerhetsmiljøet. Ingen av dem kjente identiteten til personen bak Twitter-kontoen, men flere av dem var kjent med lekkasjene og uttalte at så vidt de kjente til var informasjonen pålitelig. Vi vet fortsatt ikke hvem som sto bak Twitter-kontoen. Materialet den publiserte framsto eksplosivt. Men vi måtte faktasjekke alt før vi – eventuelt - kunne publisere.

2.4.3 Metode: IntelX

Første grep for å verifisere informasjonen var å prøve å skaffe så mye som mulig av den gjennom egne søk, og å finne den originale lekkasjen. Da kunne vi verifisere at Twitter-brukeren ikke selv hadde endret på navn og personlige opplysninger.

Som sagt foregår mye av det hackerne foretar seg på det mørke nettet. Det finne vanlige søkemotorer der også – den vanligste heter DuckDuckGo. Søk med den ga lite nyttig informasjon for oss. Det gjorde deriomt søkemotoren IntelX. IntelX går dypere, og søker ikke bare i nettsider – men finner informasjon på det mørke nettet, datalekkasjer og et utall åpne kilder. En presisering er at IntelX ikke selv hacker eller bryter seg inn på nettsider. Men den fanger opp informasjon fra datalekkasjer fra nettforum, der det kan ligge personopplysninger.

Som søkeord brukte vi e-postadresser fra de påståtte hacker-navnene som var lekket på Twitter. IntelX ga oss da materiale fra lekkasjer fra blant annet Conti og Revil: Fra sosiale medier-kontoer hackere hadde brukt fra chatteforum de hadde deltatt på og lignende. Informasjonen kom primært i tekstfiler. Ved å sammenligne det vi fant med IntelX med det som var lekket på Twitter, kunne vi slå fast at Twitter-lekkeren ikke selv hadde endre informasjonen før vedkommende publiserte den.

2.4.4 Metode: Yandex

En ting var at den skriftlige informasjonen i lekkasjene ikke var tuklet med. Vi måtte også finne ut hvorvidt personene som ble hengt ut med navn og bilde i Twitter-lekkasjene, faktisk var dem de ble påstått å være. Vi søkte opp alle bildene fra Twitter-lekkasjene i det tidligere nevnte ansiktsgjenkjenningsverktøyet Pimeyes. Vi fikk en del treff, men ikke på alle – typisk gjaldt dette fordi bildene som var lekket, ikke viste ansiktet så godt eller var tatt på lang avstand. Vi søkte opp bildene i den russiske bildegjenkjenningsmotoren Yandex, som er god på østeuropeiske kilder.

Bildesøkene avdekket at enkelte av påstandene i Twitter-lekkasjene var feil. Ett eksempel var at en påstått hacker koblet med bildet til en håpefull fra en nederlandsk datingside. På en del andre personer fikk vi ingen treff på bildesøk, verken i Pimeyes, Yandex eller Google Images. De personene ble luket ut og ikke omtalt i artikkelen om hackernes bakgrunn, da vi ikke kunne slå fast at riktig bilde av koblet til riktig person og forhistorie.

Nå kunne vi også gå igjennom sosiale medier-profiler, blogger, rekrutteringssider, Wayback Machine og annen åpent tilgjengelig informasjon for å se om informasjonen fra lekkasjene – på IntelX og Twitter – stemte med det de aktuelle personene selv oppga. Det var relevant, for eksempel for å se hvor mange av de påståtte hackerne som hadde militær erfaring. Vi grupperte navnene fra lekkasjene på Twitter og på IntelX i tre mapper – «Rødt», der vi selv hadde funnet feil i navnene. «Gult» der vi var usikre. «Grønt», der følgende stemte:

- Informasjonen fra Twitter og IntelX stemte overens
- Bildet fra Twitter stemte overens med bildene vi selv fant av de aktuelle personene
- Personopplysningene fra Twitter og IntelX stemmer med det personene selv oppgir på nett

Bare navnene i «Grønt» ble omtalt - i saken «Serverte stjernene: - Var fryktet hacker»

2.5 Hvor kom pengene fra?

Siden Killnet ikke drev med løsepengeangrep, ønsket vi å finne ut hvor de fikk penger fra.

Vi fikk en del informasjon i Killnets åpne Telegram-kanaler. I Telegram-kanalene sine ba Killnet om donasjoner – i kryptovaluta - fra støttespillere. Vi oppdaget også flere innlegg på Killnets Telegram-kanaler som var merket «sponset innhold».

Innleggene var fra Telegram-kontoen @gallernaya. I beskrivelsen på kanalens profilside sto det at det var en kanal som averterte leiligheter til salgs og utleie i St. Petersburg, og at administrator var kontoen @sergey.galler . Vi klikket oss videre inn på denne kontoen. Der fant vi en link til en Instagram-konto i navnet Sergey Galler. Gjennom Google-søk fant vi nettstedet https://www.sergeygaller.ru/ og en LinkedIn-profil som bekreftet at Sergey Galler var en eiendomsutvikler som hadde solgt og leid ut hundrevis av leiligheter i både St. Petersburg og andre byer. Vi sendte ham spørsmål både på Telegram og på Instagram. Meldingene ble merket som «lest» - men Galler svarte aldri på spørsmålene.

I Telegram-kanalene sine repostet også Killnet en musikkvideo laget av den kjente russiske rapperen Kaya Oboyma – som hadde laget en hyllestlåt til hackergruppa. Låta ble distribuert av selskapet Infinity music. På deres Youtube-kanal sto det at selskapet var grunnlagt av Bakai Kolchaev, en kirgisisk gründer som hadde bygget opp et musikkimperium. Da vi tok kontakt reagerte Bakai Kolchaev raskt – og Infinity music fjernet Killnet-låta fra sine kanaler.

2.5.1 Metode: Selskapssøk i Russland og på Kypros

Vi oppdaget også at Killnet jevnlig repostet innlegg fra en russisk smykkeprodusent: Hooliganz Jewelry, og linket til Hooliganz' side på nettsamfunnet VK – kjent som det russiske Facebook. Der averterte Hooliganz flere smykker med Killnets logo på. Videre opplyste smykkeprodusenten åpent at en del av inntektene fra smykkesalget gikk til Killnet.

Som nevnt tidligere i rapporten hadde vi kontakt med flere nåværende og tidligere medlemmer av Killnet. Vi spurte dem om samarbeidet med Killnet. En av dem, «Igor», bekreftet at smykkesalget genererte «gode inntekter» for gruppa. På VK opplyste Hooliganz at virksomheten var grunnlagt av russeren Sergej Logunov. På VK søkte vi opp hans private profil, som var full av prorussisk propaganda og latterliggjøring av NATO og Ukraina. Politisk var han dermed på linje med hva Killnet sto for. Google-søk avslørte at han tidligere hadde drevet med salg av diamanter og at han var aktiv i motorsykkelmiljøet i Moskva.

Det russiske selskapsregisteret er tilgjengelig gjennom nettsiden Rusprofile.ru. Men da vi søkte på Hooliganz i registeret, fant vi ingen treff. Vi søkte både med norske og russiske bokstaver – ved hjelp av kyrillisk keyboard hos Lexilogos: https://www.lexilogos.com/keyboard/russian.htm . Vi søkte også på Viktor Logunov. Da fant vi flere selskaper, på flere ulike personer med samme navn. Det var liftselskaper, elektronikkvirksomheter og enkeltpersonforetak, men ingen selskaper som framsto som noe smykkeselskap. Kunne selskapet være registrert et annet sted?

Vi søkte opp Hooliganz i selskapsdatabasen OpenCorporates, som søker i selskapsregistre fra en rekke land, verden rundt. Der fikk vi treff – på Kypros. Der sto Hooliganz Jewelry Ltd registrert på to personer med russiske navn – Roman Iuppa og Tamara Gushanova. Vi søkte opp disse to

personene på OpenCorporates, og oppdaget at de to hadde registrert en rekke selskaper sammen. Vi søkte dem så opp på Facebook, og oppdaget at Roman og Tamara var gift. Fra OpenCorporates var det også linket til det kypriotiske selskapsregisteret, der vi fikk verifisert at Hooliganz Jewelrys registrering på Kypros var nylig bekreftet. Vi reiste til Kypros for å snakke med ekteparet. De gjorde det de kunne for å unngå oss, og svarte heller ikke på henvendelser via kontoene deres i sosiale medier. På LinkedIn oppga Roman Iuppa at han jobbet i finansavdelingen i et stort investerings- og kryptoselskap i Limassol, mens Tamara Gushanova opplyste at hun jobbet i et eiendomsselskap i samme by som solgte luksuseiendommer til russere som ønsket kypriotisk oppholdstillatelse. Vi kontaktet begge arbeidsplassene de hadde oppgitt på LinkedIin, og reiste til landsbyen der Gushanova opplyste at paret bodde – alt uten hell.

Delvis fordi arbeidsplassen til Iuppa ville bli nevnt i saken – det var relevant å fortelle at en ansatt i Exness, et av Kypros' største investeringsselskaper, var fasilitator for finansiering av russiske hackere. Og dels fordi Iuppa selv ikke svarte, besluttet vi å kontakte Iuppas sjef. Vi søkte opp sjefen for finansavdelingen i selskapet Exness.Vi googlet «Exness email format» og fant karrieresider der e-postformatet til ansatte i selskapet var. Så sendte vi en henvendelse til Iuppa med finanssjefen Alexis Alichanidis i kopi. Da skjedde ting raskt. Dagen etter svarte Iuppa– med sjefen i kopi – og ba om dokumentasjon for anklagene.

Det kunne vi sende ham uten å dele upublisert materiale, siden koblingen mellom Iuppa/Gushanova var åpent tilgjengelig på nett, og koblingen mellom Hooliganz og Killnet var dokumentert i saken «Vi jaktet hacker-pengene: - Dra til helvete» som allerede var publisert. («Dra til helvete» var Hooliganz-grunnlegger Viktor Logunovs hilsen til oss.) Vi sendte skjermdumper fra VK-kontoene og utskrift fra selskapsregistrene. Sikkerhetssjefen i Exness kalte oss nå inn til Google Meet-møte, før det raskt ble avlyst – og vi fikk en e-post om at Roman Iuppa hadde fått sparken. Saken: Hacker-pengene leder til ektepar

2.5.2 Metode: Sporing av bitcoin-transaksjoner

Både i Killnets forespørsler om donasjoner og i dialogen med aktive og tidligere Killnet-medlemmer var det et tema som dukket opp til stadighet: Kryptovaluta, spesielt bitcoin.

Gruppa ba jevnlig om donasjoner i bitcoin, Hooliganz-smykkene med Killnet-logo kunne sågar kjøpes med bitcoin og en av Killnet-hackerne vi var i kontakt med hevdet at gruppa hadde fått et stort beløp i bitcoin etter at de var involvert i et angivelig hackerangrep mot Rutor, et darkweb-forum som var linket til ukrainsk etterretning. På Telegram sendte Killnet-hackeren «Igor» over det han hevdet var bevis for at Killnet hadde mottatt penger fra darkweb-forumet Rutor: Link til tre transaksjoner, logget på nettstedet blockchain.com.

Hackeren hevdet at transaksjonene var løsepenger etter Killnets angrep mot forumet. Vi googlet, og fant at flere sikkerhetsblogger hadde omtalt at det faktisk hadde skjedd et hackerangrep mot Rutor-forumet, at det forelå påstander om motivet var at forumet var knyttet til ukrainsk etterretning og at det skulle ha blitt betalt løsepenger til Killnet. Vi ble nysgjerrige på bitcoin-pengestrømmene til Killnet, men så samtidig egentlig ikke for oss videre graving i dem: Første innskytelse var at kryptovaluta ikke var sporbart. Vi kontaktet flere kryptoeksperter – men de fleste var negative, og bemerket: Bitcoin er designet for ikke å være sporbart. Det var Colin Boyd, professor ved NTNU, som sa: *«Det høres ut som de involverte* vil *bli sporet. For å bevise at en transaksjon fant sted.»*

Spørsmålene

Killnet-hackeren «Igor» hadde delt tre transaksjoner med oss – og mottakeradressene til disse. På sine Telegram-kanaler oppga Killnet også to bitcoin-adresser som gruppa selv opplyste at tilhørte dem. Dermed var ikke alt så anonymt likevel. Vi hadde fem bitcoin-adresser som angivelig kunne

knyttes til Killnet. Kunne vi finne en forbindelse mellom adressene som «Igor» hadde sendt oss – til adressene Killnet selv opererte med? Og selv om bitcoin går i en endeløs sirkel, kunne vi finne ut hvem Killnet samarbeidet med?

Sporingen begynner

Så vidt vi kjente til hadde ingen norske journalister tidligere klart å spore bitcoin-transaksjoner på denne måten. Vi tok utgangspunkt i nettstedet Blockchain.com. Blockchain.com er et kryptoselskap, som oppgir at de begynte – som første selskap – å loggføre bitcoin-transaksjoner i 2011. På nettstedet er alle transaksjoner klikkbare – og du kan således følge transaksjoner fra avsender X videre til mottaker Y, deretter videre til mottaker Z, X, Æ, Ø, Å og videre. I utgangspunktet er ikke dette vanskeligere enn å for eksempel følge bekjentskaper via vennelister på Facebook. Men utfordringen er at transaksjonsadressen er veldig lange – og at det ofte har gått et høyt antall transaksjoner inn og ut av hver adresse. Det gjelder dermed å følge nøye med på hvilken pengestrøm akkurat du følger. Hver transaksjon er logget med avsender, dato og klokkeslett. Klikker du på denne, kommer du videre til kontoen den er sendt til – men da får du også opp alle andre transaksjoner som har gått inn og ut av denne adressen.

Vi noterte alle overføringer i et word-dokument for å hjelpe oss å holde oversikten – og lagde et lite notat for hver overføring, med avsender- og mottageradresse, for å ikke miste oversikten. Om avsender A skal sende penger til mottaker B går heller ikke pengene direkte fra A til B. I stedet går de via mellomstopp, C, D, E, F, G osv, før de til slutt ender der de skal. Kontoene hadde navn som «bc1qng0keqn7cq6p8qdt4rjnzdxrygnzq7nd0pju8q».

Eksperten

Vi bestemte oss derfor for å finne en samarbeidspartner som kunne mer om dette enn oss. Torbjørn Bull Jenssen er en kjent norsk kryptoekspert. Han er sjef i selskapet Arcane Crypto. Han tipset oss om sin senioranalytiker Anders Helseth, som ble vår sparringpartner.

Eksempelvis: Hver konto har et felt der det står «total received» - altså hvor mye bitcoin som totalt har gått inn på en adresse. Vi trodde at dette kunne gi en indikasjon på hvor mye konto-eieren var god for. Der korrigerte Anders Helseth oss: det regnestykket ble for enkelt. Heller viste det hvor mye som hadde gått inn, men tok ikke med i beregningen hvor mye som hadde gått ut igjen. Helseth bekreftet at vår metode med å spore transaksjonene ett og ett trinn, og følge med på at vi følger rett pengestrøm – med rett avsenderadresse, rett dato og rett klokkeslett – var riktig. Vi fant at:

- Det hadde gått bitcoin fra «løsepengeadressene» og til adressene som Killnet selv oppga var deres egne. Vi kunne fortsatt ikke vite om «Igor» - Killnet-hackeren vi hadde kontakt med - snakket sant når han hevdet at dette var løsepenger fra ukrainsk etterretning. Men han snakket sant når han hevdet at den aktuelle pengestrømmen endte opp hos Killnet.

- Vi fant også to kontoer der en del av Killnets bitcoin stoppet opp – og ikke ble sendt videre. Den ene står det nesten 5000 bitcoin på nå – noe som tilsvarer 87 millioner dollar. Den andre står det snaut 60 bitcoin på nå. Totalt blir dette over en milliard kroner. Disse undersøkelsene ble saken: Oppdager skjult milliard . Hadde Killnet *så* mye penger?

Der pengene stoppet

Ved å søke opp de aktuelle kontonummerne på Twitter og på Reddit, to sosiale medier der det skrives mye om kryptovaluta, fant vi en forskningsrapport der det ene kontonummeret var nevnt – nemlig kontoen der det sto nesten 5000 bitcoin. I rapporten, og i automatiserte Twitter-meldinger fra bots som følger krypto-pengestrømmer, framgikk det at kontoen tilhørte kryptobørsen Bitfinex. En kryptobørs er en virksomhet der du kan sette kryptovaluta inn, og ta «vanlige penger» ut. Skal

du hvitvaske kryptovaluta tjent på kriminell virksomhet, om til hvite penger du kan kjøpe hus eller bil for, er en kryptobørs et smart sted å gå. Bitfinex er en av verdens største kryptobørser, og holder til på De britiske jomfruøyer. Vi kunne nå slå fast at penger fra Killnets virksomhet hadde blitt sluset inn til en av verdens viktigste kryptobørser. Dette ble saken: Hit gikk de skjulte pengene

I forskningsrapporten vi hadde funnet, framgikk det at Bitfinex-kontoen som Killnet-pengene hadde stoppet på var Bitfinex sin «hot wallet»-konto. I bitcoin-terminologien betyr «hot wallet» en konto som er tilknyttet Internett (i motsetningen til en «cold wallet», som er tatt av nett). En «hot wallet»-konto et bra sted å overføre penger, om du enten vil trade de videre – eller om du vil veksle de om og ta de ut. Undersøkelsene vi gjorde med Anders Helseth, viste at Killnet-pengene stoppet hos «hot wallet»-kontoen Bitfinex. Vi kunne ikke slå fast hva som skjedde så. Men siden bitcoinene ikke gikk videre, ble de trolig vekslet til vanlige penger.

Ukrainske myndigheter, som under president Zelenskyj har vært opptatt av kryptovaluta, tok avsløringen på stort alvor. Digitaliseringsdepartementet slo i et langt e-postintervju med oss fast at de ville «ta affære» mot det de så på «som et mulig brudd på sanksjonene mot Russland». De reagerte på vår avsløring av at en av verdens fremste kryptobørser så ut til å ha hjulpet russiske hackere med å hvitvaske penger – men hadde ikke mulighet til å utdype etter at bombardementet mot Kyiv ble gjenopptatt med angrep mot infrastruktur og strømkilder.

2.5.3 Metode: Bitcoin-klagerapporter

Da vi gjorde Google-søk på Killnets bitcoin-adresser, kom vi over nettstedet Bitcoin Abuse. Det viste seg å være en slags «Slettmeg.no» for bitcoin-adresser – der folk kunne melde inn dårlige erfaringer med spesifikke kontoer, advare andre mot adresser som ble brukt i svindel, kriminalitet og lignende. Vi søkte opp adressene fra Killnet-undersøkelsene – og fikk treff på to av dem. Nemlig de to kontoene der Killnets penger hadde stoppet opp. Der vi nå visste at en av dem var «hot wallet»-kontoen til kryptobørsen Bitfinex.

På Bitcoin Abuse så vi at det hadde kommet en rekke klager på de to adressene. Spesielt interessant var Bitfinex-adressen, siden vi siste hvem som eide den. Ifølge klagene hadde midler fra flere ulike former for svindel gått inn på «hot wallet»-kontoen til Bitfinex. Blant kundeklagene var klager på at de var misbrukt i datingsvindel og «Elon Musk-svindel» – der manipulerte videoer av milliardæren ble brukt for å svindle folk til å kjøpe falsk kryptovaluta.

Svindelselskapet

Også konkrete selskapsnavn ble nevnt i kundeklagene. Det er Finanstilsynet som fører tilsyn med antatte svindelselskaper i Norge. På deres nettsider oppdaget vi at det er mulig å søke på selskapsnavn hos dem for å finne ut om de har advart mot selskaper tidligere. Der oppdaget vi at de hadde advart mot et av dem tidligere - et selskap ved navn OTPFX. På Bitcoin Abuse kan også klagerne legge inn nasjonaliteten sin, og flere av dem oppga å være norske. Vi kunne dermed avsløre at Bitfinex sin «hot wallet»-konto så ut til å ha blitt brukt til å vaske penger fra nettsvindel i Norge. Vi merket oss likevel at opplysningene på Bitcoin Abuse stammet fra selvrapportering – og at vi måtte ha et forbehold i vår omtale.

Selskapet Finanstilsynet hadde advart mot, hadde ifølge finanstilsynet i Belgia operert med en adresse på Kypros. Den så vi i det kypriotiske selskapsregisteret at tilhørte en advokat. Vi oppsøkte ham på Kypros og intervjuet ham om selskapet, som han hevdet å ikke kjenne til. Men han bekreftet at han la til rette for selskapsregistrering. Dermed kunne vi vise hvor lett det var å registrere selskap som i Norge ble brukt til kriminell virksomhet: - Er det en bombe?

3 Spesielle erfaringer

Som omtalt i rapporten ble Amedia utsatt for et massivt hackerangrep i jula 2021. Dermed var det naturlig å kontakte dem. Vi tok derfor kontakt med Pål Nedregotten, den gang konserndirektør for IT i Amedia, og han uttaler seg i saken vi publiserte – der det blant annet går fram hvilken hackergruppe som angrep Amedia og hvilke forbindelser disse har til hackergruppa Conti. Conti antas å ha forbindelser til russisk etterretning.

I sitatsjekken ba Nedregotten om å få hele manuset tilsendt. Dette er noe kilder spør om med jevne mellomrom, men som regel ikke noe som innvilges. I enkelttilfeller, spesielt med utsatte kilder i betente saker, lar vi dem likevel få lese hele manus i sitatsjekken. Vi understreket overfor Pål Nedregotten at vi ikke gjør dette i alle saker, og i hvert fall ikke i saker som angår konkurrenter. Derfor var vi klare på at dette var mellom oss og ham.

- Når publiserer dere?» spurte Nedregotten, klokka 22.34 søndag 26. juni. Vi svarte at terrorangrepet i Oslo forsinket publiseringen, men at vi håpet på den kommende uka. Før vi hadde publisert, sendte Amedia så pressemelding om hvem som sto bak hackerangrepet.

Sikkerhet

Fra en stor virksomhet som tidligere hadde gått ut i media og gikk store mengder informasjon om hackerangrepet de ble utsatt for, kom det nå tilbakemeldinger på at dette hadde medført sikkerhetsrisikoer for dem. Vi holdt derfor tilbake en del detaljer.

Av hensyn til egen sikkerhet hadde vi en egen PC øremerket til darkweb – og bare det. Dette for å hindre at PCen kunne brukes til å infiltrere Dagbladets systemer. Vi varslet IT-avdelingen i forkant av hver større publisering, så de kunne iverksette ekstra Ddos-beskyttelse av DB.no. Både NRK og VG ble angrepet under Killnet-angrepet mot Norge i juni. All kommunikasjon foregikk kryptert, på Signal og Telegram samt via Protonmail. I kontakten med medlemmer av Killnet delte vi aldri informasjon som kunne bidra til å identifisere andre hackere. Vi antok at det kunne foreligge sikkerhetsrisiko for personer som var i kontakt med et vestlig medium.

4 Konsekvenser

FANT NYTT MØNSTER: - Forskningssjefen på NUPI mener bitcoin-avsløringene våre viser et nytt operasjonsmønster for russiske hackergrupper. Espen Johansen, CSO i Visma og en av Norges fremste cybereksperter, slo fast: «Viktigheten av pressens rolle i å tydeliggjøre kriminalitetens omfang og metoder står for meg som mye tydeligere etter å ha lest deres artikler».

REGJERINGEN SLO FULL ALARM: - Norske myndigheter slo full alarm da vi avslørte at Killnet angrep Norge. Verken Arbeidstilsynet eller NAV visste hva som hadde skjedd før Dagbladet ringte. Det var statsministeren og NSM-sjefen selv som gikk ut da faren var over.

UKRAINA TOK AFFÆRE: - Ukrainas regjering reagerte kraftig på avsløringene våre om at russiske hackere kunne overføre bitcoin og tilsynelatende hvitvaske penger, via den kjente kryptobørsen Bitfinex. Ukraina varslet at de vil ta affære for å rydde opp.

NYE ETTERFORSKNINGSSKRITT: - Kripos fattet interesse for våre undersøkelser av hackerangrepet mot det norske rederiet Vard. Etter våre funn, foretok Kripos seg nye etterforskningsskritt i saken for å undersøke mulig betaling av løsepenger.

KUTTET BÅND: - En russisk finansmann som bisto Killnet i å tjene penger, fikk sparken.
En låt av der kjente russiske rapartisten Kaje Oboyma erklærte sin støtte til Killnet, ble fjernet fra plattformene til produksjonsselskapet Infinity Music.

Vedlegg: Artikkelliste

14. april: Russisk cybervåpen funnet i Norge
https://www.dagbladet.no/nyheter/russisk-cybervapen-funnet-i-norge/75858022

5. mai: Nordmannens rolle blant Putins nærmeste
https://www.dagbladet.no/nyheter/nordmannens-rolle-blant-putins-naermeste/75933410

6. mai: Støtter invasjonen av Ukraina
https://www.dagbladet.no/nyheter/stotter-invasjonen-av-ukraina/75940979

7. mai: Ukraina varslet PST om nordmann
https://www.dagbladet.no/nyheter/ukraina-varslet-pst-om-nordmann/75989135

9. mai: Eksperter: I Russlands interesse
https://www.dagbladet.no/nyheter/eksperter-i-russlands-interesse/75941329

24. juni: Sporene fra Hurtigruten-angrepet
https://borsen.dagbladet.no/nyheter/sporene-fra-hurtigruten-angrepet/76366372

18. juni: Dataangrep mot Nordland fylkeskommune: - Angrepet fra utlandet
https://www.dagbladet.no/nyheter/angrepet-fra-utlandet/76352678

19. juni: Mottok russisk hedersmedalje
https://www.dagbladet.no/nyheter/mottok-russisk-hedersmedalje/76339399

28. juni: Mystisk angriper: - Jobber med spiongruppe
https://www.dagbladet.no/nyheter/mystisk-angriper-jobber-med-spiongruppe/76410313

29. juni: Russiske hackere angriper Norge
https://www.dagbladet.no/nyheter/russiske-hackere-angriper-norge/76487161

29. juni: Truer familien til Jens
https://www.dagbladet.no/nyheter/truer-familien-til-jens/76487713

29. juni: Hacker til Dagbladet: - Vi planla angrepet
https://www.dagbladet.no/nyheter/hacker-til-dagbladet-vi-planla-angrepet/76489112

29. juni: Hackergruppe ga stoppordre: Dette skjedde
https://www.dagbladet.no/nyheter/hackergruppe-ga-stoppordre-dette-skjedde/76352164

1. juli: Ukjent e-post før angrepet
https://www.dagbladet.no/nyheter/ukjent-e-post-for-angrepet/76489649

5. juli: Hackerangrep mot Posten: - Bruk brevdue neste gang!
https://www.dagbladet.no/nyheter/bruk-brevdue-neste-gang/76536396

25. august: Russiske støyangrep mot Norge: - Farlig
https://www.dagbladet.no/nyheter/russiske-stoyangrep-mot-norge-farlig/76931632

28. august: Her er Killnet i Norge
https://www.dagbladet.no/nyheter/her-er-killnet-i-norge/76940440

1. september: Russere angrep vannsystemet i Drammen
https://www.dagbladet.no/nyheter/russere-angrep-vannsystemet-i-drammen/76507484

4. september: Advarer Norge mot russisk tokt
https://www.dagbladet.no/nyheter/advarer-norge-mot-russisk-tokt/77040225

28. september: Da hackerne slo til: - Fikk helt noia
https://www.dagbladet.no/nyheter/da-hackerne-slo-til-fikk-helt-noia/77165284

4. oktober: Ante ingenting før angrepet: - Dette skjer ikke
https://www.dagbladet.no/nyheter/ante-ingenting-for-angrepet-dette-skjer-ikke/77236564

6. oktober: Bygget norske spionskip: Hacket av russere
https://www.dagbladet.no/nyheter/bygget-norske-spionskip-hacket-av-russere-1/77280247

14. oktober: Eldre og barnevernsbarn rammet
https://www.dagbladet.no/nyheter/eldre-og-barnevernsbarn-rammet/77146088

16. oktober: Vi jaktet hacker-pengene: - Dra til helvete
https://www.dagbladet.no/nyheter/vi-jaktet-hacker-pengene-dra-til-helvete/77167375

23. oktober: - Jeg angrep Norge
https://www.dagbladet.no/nyheter/jeg-angrep-norge/76997694

13. oktober: Hackernes favorittmål i Norge
https://www.dagbladet.no/nyheter/hackernes-favorittmal-i-norge/77704079

19. november: Hacker-pengene leder til ektepar
https://www.dagbladet.no/nyheter/hacker-pengene-leder-til-ektepar/77632007

22. november: Oppdager skjult milliard
https://www.dagbladet.no/nyheter/dagbladet-avslorer-oppdager-skjult-milliard/77456456

30. november: Hit gikk de skjulte pengene
https://www.dagbladet.no/nyheter/hit-gikk-de-skjulte-pengene/77793028

2. desember: - Er det en bombe?
https://www.dagbladet.no/nyheter/er-det-en-bombe/77818756

4. desember: Ukrainas regjering etter Dagbladet-avsløring: - Vil ta affære
https://www.dagbladet.no/nyheter/vil-ta-affaere/77885045

8. desember: Eksperter etter Dagbladet-avsløringer: Ser russisk endring
https://www.dagbladet.no/nyheter/ser-russisk-endring/77730360

25. desember: Serverte stjernene: - Var fryktet hacker
https://www.dagbladet.no/nyheter/serverte-stjernene-var-fryktet-hacker/77953721

14. januar: Støttet hackere: - Fjernes
https://www.dagbladet.no/nyheter/stottet-hackere-fjernes/78204861

Samleside for sakene her: https://www.dagbladet.no/emne/sporene_til_russland . (Den eneste som ikke ligger der er Hurtigruten-saken, som ble publisert hos Børsen - link i oversikten over.)

Disse har også bidratt til rapporten:
Christina Korneliussen (TV), Nina Hansen (foto og video), John T. Pedersen (foto), Kristian Ridder-Nielsen (foto), Paul Sigve Amundsen (foto), Siri Gedde-Dahl, gravesjef

Journalistene Andrei Soshnikov, Ola Strømman, Siri Wiersen, Frode Andresen, Tharald Halvorsen, Emma Victoria Hegnar, Madeleine Hatlo, Leif Stang, Oleg Grabenko, Oda Ording, Emma Sofie

Sørli, Jon Even Andersen, Brage Lie Jor og Marthe Småkasin Lien bidro på enkeltartikler og i livedekning av hackerangrepet mot Norge 29. juni.

Forsidebilde:
F.v.: Killnet gjorde narr av utenriksminister Anniken Huitfeldt da de angrep Norge i juni – det russiske ekteparet som registrerte et smykkeselskap som samarbeidet med Killnet – den antatte Conti-hackeren «Wazawaka» - en Killnet-tilhenger fotografert i Oslo – luksusbilene til hackerne som angrep Hurtigruten. Foto: Scanpix/privat