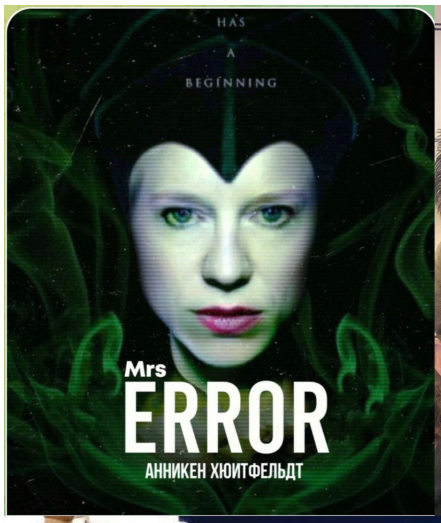
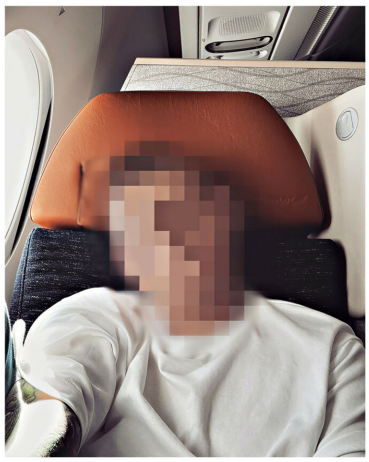
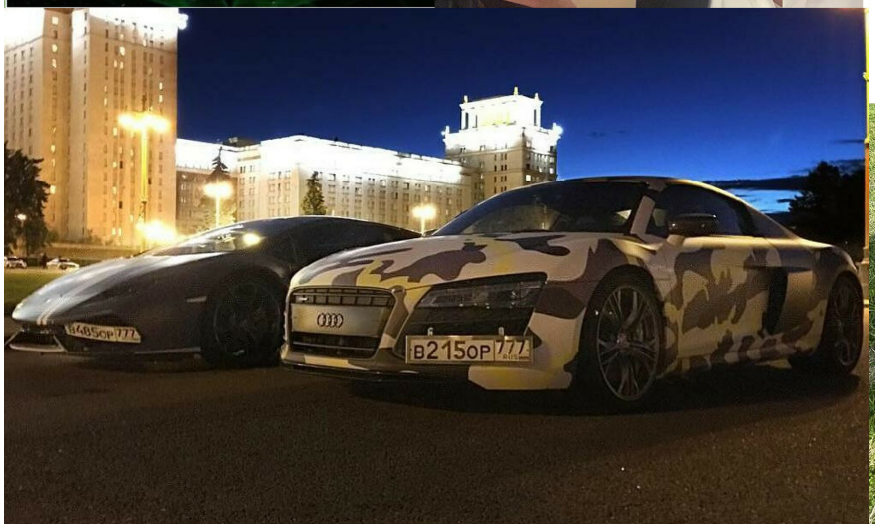
Sporene til Russland







Metoderapport SKUP 2022

Dagbladet

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

Disse leverer rapporten:
Journalister: Torgeir P. Krokfjord og Thomas Frigård

Disse har også bidratt:
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

Oslo, 15. januar 2023

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

INNHOLD

1 Innledning ... 1
1.1 Dagbladet har avslørt ... 1
1.2 Innledning ... 2
1.3 Problemstillingen tar form ... 2
1.4 Tidsbruk ... 2
2 Metode ... 3
2.1 Metode: Sikkerhetsblogger ... 3
2.2 Metode: Det mørke nettet ... 3
2.3 Metode: Kontakte ofrene ... 4
2.4 Metode: Einnsyn ... 4
2.5 Metode: Eksperter ... 5
2.6 Metode: Innsyn hos Luftfartstilsynet og Nkom ... 6
2.7 Angrepet mot Norge ... 6
2.7.1 Metode: Telegram ... 6
2.7.2 Metode: Folkeregisteret ... 7
2.7.3 Metode: Innsyn hos Sysselmesteren ... 8
2.8 Hvem er hackerne? ... 8
2.8.1 Metode: Personsøk i Telegram ... 8
2.8.2 Metode: Pimeyes ... 10
2.8.3 Metode: IntelX ... 11
2.8.4 Metode: Yandex ... 11
2.9 Hvor kom pengene fra? ... 12
2.9.1 Metode: Selskapssøk i Russland og på Kypros ... 13
2.9.2 Metode: Sporing av bitcoin-transaksjoner ... 14
2.9.3 Metode: Bitcoin-klagerapporter ... 17
2.10 Hendrik Weber ... 17
2.10.1 Metode: Russiske selskapssøk del 2 ... 18
2.10.2 Metode: Innsyn i kommuneforslag ... 18
3 Spesielle erfaringer ... 18
3.1 Kontakten med Amedia ... 18
4 Sikkerhet og etikk ... 19
4.1 Sikkerhet ... 19
4.2 Etikk ... 19
5 Konsekvenser ... 20

1 Innledning

1.1 Dagbladet har avslørt

- Dagbladet avslørte 29. juni at den russiske hackergruppa Killnet angrep norske myndigheter og medier: Arbeidstilsynet, NAV, politiet, VG, NRK, Difi, BankID og flere andre virksomheter. Kommunikasjonsstaben i Nasjonal sikkerhetsmyndighet var ikke klar over angrepet da vi kontaktet dem for kommentar.
- Dagbladet avslørte at gruppa kom med grove trusler mot Jens Stoltenberg og hans familie, og at gruppa hevdet å ha en kopi av Stoltenbergs pass. Vi avslørte at passet ikke var ekte.
- Dagbladet avslørte at den russiske hackergruppa Killnet har sendt penger gjennom den kjente kryptobørsen Bitfinex på De britiske jomfruøyer. Ukrainas regjering mener dette er hvitvasking av penger.
- Dagbladet avslørte 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.
- Dagbladet og Kommunal Rapport kartla 49 hackerangrep mot norske bedrifter de to siste årene, og avslørte at hackergrupper fra Russland står bak nesten sju av ti av dem.
- Dagbladet og Kommunal Rapport avslørte identiteten og bakgrunnen til et tosifret antall medlemmer av de beryktede, russiske hackergruppene Killnet, Conti og Revil. Vi avslørte at flere av dem hadde militær bakgrunn fra det russiske forsvaret.
- Dagbladet og Kommunal Rapport avslørte at gründeren bak et populært russisk smykkemerke, og en profilert russisk eiendomsmagnat, begge aktivt hjalp til med å finansiere operasjonene til hackergruppa Killnet, som ser på seg selv som en del av «den russiske cyberarmeen».
- Dagbladet og Kommunal Rapport avslørte at et russisk ektepar bosatt på Kypros, der mannen var en erfaren russisk finansmann, sto bak et smykkeselskap som ble brukt til å generere penger til Killnet. Avsløringen førte til at finansmannen fikk sparken.
- Dagbladet avslørte at rederiet Vard, som produserer den norske etterretningstjenestens spionskip, ble hacket av en hackergruppe der flere medlemmer har fortid i det russiske forsvaret.
- Dagbladet og Kommunal Rapport avslørte at russiske hackere brøt seg inn i vannsystemet til Drammen kommune, kort tid etter at hackere forsøkte å forgifte drikkevannet til 15 000 i USA. Kommunen satte selv de to hendelsene i sammenheng.
- Dagbladet og Kommunal Rapport avslørte at det aldri har vært flere russiske «støyangrep» - jamming av GPS-signaler på norske flyplasser – enn i 2022. Det til tross for at daværende statsminister Erna Solberg i 2020 sa at hun hadde fått bukt med problemet gjennom «stille diplomati».
- Dagbladet avslørte at en profilert norsk lokalpolitiker, Hendrik Weber, hadde langt tettere forbindelser til Vladimir Putins russiske regime, enn det som var tidligere kjent. Vi avslørte at Weber kan knyttes direkte til flere av Vladimir Putins mest betrodde menn på den okkuperte Krim-halvøya i Ukraina.
- Dagbladet avslørte at Weber, samtidig som han var en profilert representant for Rødt, frontet den kjente norske politikeren en venneorganisasjon på Krim-halvøya – som støtter invasjonen av Ukraina.
- Dagbladet avslørte at den prorussiske Rødt-politikeren Weber ble hedret med en vennskapsmedalje av den russiske viseutenriksministeren Aleksandr Grusjko.
- Dagbladet avslørte at Hendrik Webers prorussiske aktivitet var av et sånt omfang og nivå at Ukraina varslet PST om den norske politikeren.

1.2 Innledning

2022 startet som et vanlig år. For oss ikke-kinesere var corona-pandemien til og med over. I gravegruppa diskuterte vi ideer, og tok opp et spennende prosjekt som hadde ligget på vent. Nyårsfreden varte fram til 24. februar. Da invaderte Russland Ukraina og endret verdensordenen. Det påvirket selvsagt også våre prioriteringer.

Nyhetsledelsen ga beskjed om at de ønsket graving i temaer som var relatert til Russland. Det kjentes naturlig: Putins Russland hadde gått fra å være en stor nabo Norge hadde et relativt ryddig forhold til, til å bli aggressoren bak det som så ut som starten på tredje verdenskrig.

1.3 Problemstillingen tar form

Etter å ha diskutert flere innganger, falt vi ned på at vi ønsket å undersøke russisk aktivitet i Norge – og cyberaktiviteten spesielt. Tre måneder tidligere hadde Amedia – et stort konsern i vår egen bransje – blitt angrepet av hackere. Samme vinter hadde også NRK og DN hatt store saker på et antatt russisk-linket hackerangrep mot Choice Hotels. Vi ønsket å finne ut hvor mange slike angrep norske virksomheter var utsatt for. Og ikke minst: Hvem var de, hackerne som angrep norske myndigheter og bedrifter, som skal ha tjent hundrevis av millioner i løsepenger, som gjorde at ansatte i vanlige norske bedrifter og kommuner skulle fortelle oss at de ble sykmeldt og livredde?

Vi formulerte tre hypoteser:

- Hvor mange norske virksomheter er angrepet?

- Hvem er hackerne?

- Hvordan finansierer de virksomheten sin?

Samtidig var gravemiljøet i Dagbladet presset– vi bisto i den løpende krigsdekningen, og diskuterte andre større prosjekter samtidig. Nyhetsavdelingen jobbet døgnet rundt med invasjonen. Var det folk utenfor vår egen redaksjon som kunne bistå? Vi var kjent med Thomas Frigårds navn fra tidligere – gjennom hans gode gravejournalistikk over flere år.

Siri Gedde-Dahl kontaktet Kommunal Rapport, og Dagbladets gravegruppe møtte Kommunal Rapports redledelse og reporter Thomas Frigård til et møte. Redaksjonene hadde sammenfallende interesser – men ble enige om at alle saker ikke trengte å bli publisert begge steder. Thomas Frigård fra Kommunal Rapport skulle sitte hos Dagbladet i tre måneder. Ved publisering av de første hacker-avsløringene sendte vi ut pressemelding.

Tanken bak prosjektet var løpende publisering, og saker ble publisert fortløpende fra juni fram til nyttår. Vi trodde ikke at vi kunne slå de russiske hackerne på det mørke nettet, på programmering og IT-teknisk kompetanse. Men kunne vi avsløre dem med åpne kilder? Jo lenger vi kom ned i materien, jo mer kreative måtte vi være i metodebruken. Jo mer vi fant ut, jo vanskeligere ble det å finne ut enda mer - og jo større krav stilte det til metodebruken vår. Men jo mer vi fant ut – desto mer givende var det å grave videre.

1.4 Tidsbruk

Torgeir P. Krokfjord jobbet med prosjektet fra slutten av april fram til jul, delvis parallelt med et annet graveprosjekt, og reportasjeledet også prosjektet mesteparten av tida. Thomas Frigård jobbet med prosjektet på et tre måneders vikariat (juni, august og september), delvis parallelt med andre oppgaver. Reportere på nyhetsavdelingen og utvikler Ola Strømman bisto på enkeltartikler, spesielt under dataangrepet mot Norge 29. juni.

2 Metode

Hvem er hackernes norske ofre?

Hvert år publiserer Teknisk Ukeblad en liste over hackerangrep i Norge. Vi tok utgangspunkt i denne da vi skulle kartlegge hackerangrep mot norske virksomheter. Men vi kunne ikke umiddelbart slå oss til ro med at TU sin ellers gode oversikt inneholdt alle angrep. Delvis fordi TU i stor grad baserte lista si på medieomtale, og dermed ikke tok med angrep der ofre og/eller angriper ønsket å holde hackerangrepet skjult. Og dels fordi lista, selv i saker der ofrene var kjent, ikke alltid inneholdt navn på angriperne.

Vi måtte derfor bruke andre kilder for å finne ut om det var flere ukjente hackerangrep mot norske virksomheter – og finne gjerningspersonene i så mange av de kjente angrepene som mulig.

2.1 Metode: Sikkerhetsblogger

Dette gjelder både statlige grupper, som Fancy Bear – gruppa som, ifølge PST, i 2020 angrep Stortinget. Og det gjelder såkalte løsepengehackere – som Conti, Revil, Evil Corp, Lockbit og Hive. Fra tidligere medieomtale var det kjent at både Nortura, Choice Hotels og andre norske virksomheter var angrepet av slike hackere. Gruppenes modus har vært å infisere ofrenes datasystemer og enten hente ut materiale – eller påstå at de har gjort det. For så å så kontakte ofrene selv og informere om at de er hacket. Ofrene kan så få en «forsmak» på materialet hackerne har stjålet, med beskjed om at om de ønsker å få materialet tilbake må de betale en større sum i bitcoin.

Det finnes en rekke cybersikkerhetsselskaper som lever av å hjelpe ofrene for slike hackerangrep, og derfor følger hackergruppene tett. Flere av dem publiserte jevnlig nye og oppdaterte oversikter over angrepene. På Twitter kom vi over kontoen til selskapet **Dark Tracer**. De leverer i utgangspunktet betalingstjenester, men publiserer med ujevne mellomrom en større oversikt over dataangrep på det åpne nettet, basert på deres granskning av hackergruppenes aktivitet på det mørke nettet. På Twitter-kontoen sin delte de en gratis oversikt over nesten 2700 hackerangrep – med navn på hvilken gruppe som hadde tatt på seg ansvaret for hackerangrepet,

En lignende tjeneste leveres av sikkerhetsselskapet HackNotice. På Facebook står de bak en automatisert tjeneste som overvåker hackergruppene. Vi gikk igjennom alle innlegg fra HackNotice-feeden tilbake til januar 2020. Ved å gjennomgå kartleggingene til DarkTracer og HackNotice, fant vi både angrep mot norske virksomheter som ikke var tidligere kjent – og vi fant de antatte hackerne bak norske angrep der dette ikke var omtalt før. Disse listene kunne danne utgangspunktet for undersøkelsene våre. Men vi ønsket å verifisere dem før vi publiserte.

2.2 Metode: Det mørke nettet

Vi ønsket også, så langt det var mulig, å ettergå hva hackergruppene selv opplyste om de norske angrepene. Det var lettere sagt enn gjort.

Vi hadde i bransjeartikler og annen medieomtale kommet over den amerikanske sikkerhetsanalytikeren Brett Callow. Vi tok kontakt med ham på forsommeren 2022, og gjorde et intervju om de russiske løsepengehackerne. Han påpekte at korrespondansen mellom offer og hacker gjerne foregår på det mørke nettet, der hackergruppene ofte har hatt en egen side eller blogg.

Callow fortalte at flere av disse var nå offline – etter en del arrestasjoner vinteren 2021/22 og politiske bruduljer etter invasjonen av Ukraina. Da vi begynte researchen for alvor i mai 2022, var det ifølge Callow bare hackergruppene Lockbit og Hive som fortsatt hadde operative blogger.

Det mørke nettet – darkweb på engelsk – er kanskje mest kjent for at det der finnes forum der du kan få kjøpe bortimot hva det skal være av ulovlige varer: narkotika, våpen, ID-papirer og det meste annet. Det finnes også en rekke «hvite» tilbud der, som fungerer omtrent som det vanlige Internett med søkemotorer og sider med informasjon. Men på det mørke nettet er det lettere å skjule hvem du er – om det er det du vil – og derfor var det her hackergruppene hadde sine blogger.

Fra Brett Callow fikk vi url-ene til bloggene til Hive og Lockbit. På bloggene fant vi at de hadde publisert informasjon om angrep mot flere norske ofre. Denne informasjonen indikerte at det vi hadde funnet ut om deres norske ofre, som Amedia, CGM og GK Entreprenør, var riktig. Fordi hackerne selv bekreftet uavhengige opplysninger om koblingen mellom hackergruppe og offer.

Etter at vi hadde samlet inn en ny og mer omfattende liste over norske ofre – basert på informasjonen fra DarkTracer, HackNotice, Teknisk Ukeblad og fra hackergruppene selv, hadde vi nå en liste på 49 norske ofre for russiske hackergrupper.

2.3 Metode: Kontakte ofrene

Vi formulerte en e-post som gikk til samtlige av de antatte norske ofrene. Den ble tilpasset litt utfra hver sak, men i hovedtrekk lød den slik:

> *«Hei du!*
>
> *Vi i Dagbladet har så vidt begynt på et større prosjekt der vi ser på russiske hackerangrep og angrep mot sentral infrastruktur i Norge. Et viktig element her er hackerangrep mot næringslivet – der dere som kjent har vært rammet. Vi lurte på: Hadde det vært mulig med et bakgrunnsmøte der vi gikk i detalj gjennom deres sak?*
>
> *Vi skal ikke gjøre noe intervju på det møtet, det er research og informasjonsinnhenting (vi gjør selvsagt gjerne et intervju/reportasje seinere) – for å gå igjennom situasjonen dere sto i? Vi har kartlagt en rekke lignende tilfeller, tanken er å prøve å komme nærmere hvem som står bak dette – om det er koordinert – hva som er målene osv.*
>
> *Hadde det vært mulig med et bakgrunnsmøte om deres sak?»*

Viljen til å møte oss og snakke om hackerangrepene viste seg å være liten. Noen av virksomhetene anså seg ferdige med saken, andre sa de hadde slettet det som var av interessant informasjon. Noen få gikk med på å møte oss, men mange av virksomhetene var redde for å snakke.

Vi fikk imidlertid kontakt med samtlige av de 49 ofrene som nå sto på lista vår, og fikk – on eller off record – bekreftet fra alle at de faktisk hadde vært utsatt for et hackerangrep. Det var det aller viktigste. Nå visste vi at informasjonen i vår liste over ofre var korrekt. Ofrenes historier ble sakene: Da hackerne slo til: - Fikk helt noia og Ante ingenting før angrepet: - Dette skjer ikke.

2.4 Metode: Einnsyn

Vi gjorde søk på Einnsyn på «dataangrep», «hacking» og navn på konkrete hackergrupper. Der fant vi et såkalt etterretningsnotat fra KommuneCsirt - Nasjonalt senter for informasjonssikkerhet for kommunesektoren. I notatet, som ble sendt til alle kommunene som var tilsluttet KommuneCsirts oppfølgingsprogram, slo senteret alarm om et alvorlig dataangrep mot et vannverk i Florida.

KommuneCsirt skrev også at det samtidig var «en pågående sikkerhetshendelse hos en norsk kommune». I Retriever fant vi omtale i lokalaviser av at det i februar, da KommuneCsirt sendte ut notatet, hadde vært et dataangrep mot Drammen kommune. Vi jobbet videre med kilder som kjente til angrepet, og fikk bekreftet at det var hackergruppa Avaddon som sto bak. Ifølge flere

sikkerhetsblogger hadde denne relativt lite omtalte gruppa også forbindelser til russiske hackere Dermed kunne vi trekke linjene fra et dataangrep i USA til et dataangrep mot Drammen kommune.

Forskningstoktet

Reporterne Frode Andresen og Tharald Halvorsen på nyhetsavdelingen hadde parallelt med vår jobbing undersøkt andre spor knyttet til Russland. Andresen hadde søkt systematisk på Einnsyn etter dokumenter som belyste forholdet mellom Russland og Norge. Søkeordene var «Russland», «Russia», «Ukraina», «Ukraine», «ambassade og «embassy». Søkeresultatene sorterte han etter sist publisert, før han ba om innsyn i relevante dokumenter.

Slik kom han over et dokument sendt fra Utenriksdepartementet til Russlands ambassade i Norge, hvor Utenriksdepartementet opplyste at de tillot Russland å gjennomføre et forskningstokt med forskningsfartøyet «Akademik Sergey Vavilov». Dokumentet ble før publisering forelagt en ekspert som bisto oss med å vurdere opplysningenes grad av vesentlighet.

2.5 Metode: Eksperter

23. februar 2022 publiserte Storbritannias nasjonale datasikkerhetssenter NCSC, i samarbeid med flere statlige IT- og sikkerhetsaktører, en risikoanalyse av en ny hackerprogramvare de hadde oppdaget. Skadevaren ble knyttet til russisk etterretning. Det var først og fremst nettverksrutere fra WatchGuard og Asus som er rammet.

6. april kunngjorde USAs justisdepartement at de hadde gitt deres føderale etat FBI tillatelse til å gå inn og fjerne denne skadevaren på «over 1000 infiserte enheter verden over». Tharald Halvorsen tok kontakt med Norges sikkerhetsmyndighet NSM og spurte om skadevaren var fanget opp i Norge, men NSM ville hverken bekrefte eller avkrefte om FBI hadde gått inn og fjernet skadevaren fra enheter i Norge, ei heller om de hadde registrert tilfeller av den. NSM svarte bare at de var «kjent med situasjonen». FBI svarte ikke våre henvendelser. Vi kontaktet i stedet cybersikkerhetsorganisasjoner som Shadowserver, som hadde sporet skadevaren i verden. De bekreftet at de hadde registret 210 nettverksrutere som kunne ha vært utsatt i Norge.

Vi tok derfor kontakt med norske selskaper som vi gjennom nettsøk fant at hadde levert selskaper til WatchGuard – Dustin og Absec - og spurte om de var varslet om den potensielle faren. Norske leverandører av nettverksrutere bekreftet at de var blitt kontaktet, i forbindelse med FBI-aksjonen. Dagbladet presenterte funnene til en rekke IT- og sikkerhetsaktører i Norge, og fikk bekreftet at NSM var varslet om flere enheter som var infisert med russisk skadelig programvare i Norge.

STØYANGREP: Her demonstrerer det russiske forsvaret hvordan en R-330Zh Zhitel-jammer kan brukes til å blokkere GPS-signaler. Foto: Det russiske forsvarsdepartementet / mil.ru / Wikimedia Commons

2.6 Metode: Innsyn hos Luftfartstilsynet og Nkom

Det har tidligere framkommet i mediene at luftfarten, de siste årene, har meldt om fly som mister sine GPS-signaler over norsk territorium, noe som betyr at flyene mister sitt satellittbaserte navigasjonssystem. Selv om flyene har alternative navigasjonssystemer, blir dette betegnet som et alvorlig sikkerhetsavvik. Norske myndigheter har konkludert med at forstyrrelsene kommer fra russiske kilder, og i 2020 uttalte daværende statsminister Erna Solberg at Norge gjennom «stille diplomati» hadde klart å redusere russisk blokkering av GPS-signaler over norsk territorium.

Dagbladet og Kommunal Rapport ønsket å kartlegge utviklingen av GPS-blokkering over norsk luftrom, og vi ønsket blant annet å se om det var mulig å spore en endring av GPS-blokkeringene etter Russlands angrep på Ukraina.

Alle sikkerhetsavvik i norsk luftfart blir rapportert inn til Luftfartstilsynet, og av Nasjonal kommunikasjonsmyndighet (Nkom). Ved bruk av offentlighetslovens §9 «Rett til å kreve innsyn i ei samanstilling frå databasar», ba vi Luftfartstilsynet om en oversikt over samtlige registrerte GPS-blokkeringer over norsk luftrom de siste ti år. I oversikten ba vi om å få opplyst om tid, sted, flyrute og avvikmeldingens innhold. Etter å ha klaget på manglende svar på innsynskravet, oversendte Luftfartstilsynet den ønskede oversikten etter 15 virkedager. Innsynet gjorde at vi kunne lage en tabell over antall GPS-jamminger over norsk jord, hvor omtrent hendelsene skjedde, og når.

Oversikten viser at på 178 flygninger har flyene mistet sine GPS-signaler de siste fem årene, og 106 av tilfellene er registrert i Øst-Finnmark. Det betyr at 75 prosent av sikkerhetsavvikene har skjedd i luftrommet nær den russiske grensen. Nå kunne vi lage en egen statistikk. Oversikten viste at GPS-jammingene startet med fire tilfeller i 2017, at de økte fra 30 i 2019 til 37 i 2020. Dataene fra Luftfartstilsynet viser at omfanget av GPS-jamming aldri har vært så stort som i 2020. Erna Solbergs uttalelser i desember 2020 harmonerte dermed ikke med Luftfartstilsynets data.

Vi kontaktet også Nasjonal kommunikasjonsmyndighet (Nkom), og det viste seg at de satt med mer oppdaterte tall for 2022 enn det Luftfartstilsynet hadde. Vi ba derfor om en tilsvarende oversikt fra Nkom for 2022 fram til august, mens Luftfartstilsynet kun hadde data fram til juni. Oversikten Nkom viste også at omfanget av GPS-jamming i Norge hadde «eksplodert» etter invasjonen av Ukraina. Før angrepet på Ukraina i slutten av februar 2022 hadde Nkom registrert fire tilfeller av GPS-bortfall, mens de fire siste månedene etter Russlands angrep var det registrert 27 tilfeller. Ifølge Nkom har hyppigheten aldri vært høyere enn i denne firemåneders-perioden. Dette viste vi i saken: Russiske støyangrep mot Norge: - Farlig.-

2.7 Angrepet mot Norge

2.7.1 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 helpolitisk aktør. Killnet opererte flere kanaler på Telegram som

delvis fungerte som rene propagandakanaler. De postet memes, videosnutter og manipulerte bilder som latterliggjorde Ukraina, Vesten og NATO, og framhevet de russiske invasjonsstyrkene – til sine over 30 000 følgere på Telegram.

Killnet publiserte også fortløpende hvem de selv angrep. Og i noen tilfeller annonserte de angrepene sine på forhånd. Med tanke på at Norge leverte våpen til Ukraina, og er et av de vesteuropeiske nabolandene til Russland, var det interessant å se om det også kunne komme et angrep mot Norge.

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. En morgen, ei uke seinere, endret den planen radikalt.

TRUER JENS STOLTENBERG: Men passet Killnet la ut bilde av, er falskt.

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. Da vi sjekket Arbeidstilsynets nettsider, var de 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 seinere i rapporten fikk vi kontakt med en av Killnet-hackerne. Han hevdet i et intervju med oss at angrepet var motivert direkte av norsk innenrikspolitikk – og konsekvensene denne fikk for Russland. Hackeren opplyste at Killnet angrep Norge, fordi norske myndigheter stanset godstransport fra Russland til Barentsburg på Svalbard.

2.7.2 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 relativt raskt tilbake til oss med en kommentar: Passet er falskt. Det stemte med det vi hadde funnet ut i Folkeregisteret.

Vi nådde Stoltenbergs kone på telefon – men hun la på da vi presenterte oss. Vi forsøkte også arbeidsgiverne til Stoltenbergs barn, uten hell. Etter å ha gitt alle muligheten til å kommentere, publiserte vi saken om at Killnet truet den norske NATO-sjefen og hans familie.

2.7.3 Metode: Innsyn hos Sysselmesteren

Samtidig som vi avslørte angrepet og dekket det løpende på nett, TV og papir, hadde reporter Siri Wiersen på nyhetsavdelingen fanget opp en artikkel fra E24, som omhandlet at nettopp syv tonn mat til Svalbard ble stoppet på Storskog, og at Russland krevde at maten skulle få passere. Dette var leveransen Killnet-hackeren pekte på overfor oss.

Dagbladet ba Sysselmesteren på Svalbard onsdag 29. juni om innsyn i et brev som E24 viser til i sin sak, samt all tilhørende korrespondanse. Raskt mottok vi åtte brev, hvorav det kom fram at Sysselmesteren og Utenriksdepartementet hadde vært i dialog med daværende generaldirektør i Trust Arktikugol, Akeksandr Veselov. Denne dialogen omhandlet godstransport fra Russland til Barentsburg, som ble stanset ved grenseovergangen på Storskog.

Vi visste ikke hvorvidt Killnet hadde vært i kontakt med russiske myndigheter – både hackerne og Russlands ambassade sa at dette ikke var tilfelle. Men e-posten dokumenterte at det hadde vært kontakt mellom Norge og Russland dagen før angrepet, og viste at Killnet i hvert fall hadde respondert raskt på den norske innenrikspolitiske handlingen. Saken: Ukjent e-post før angrepet.

2.8 Hvem er hackerne?

På nett bruker hackergruppene pseudonymer, de kommuniserer på det mørke nettet – gjemt bak VPN-løsninger, kryptert kommunikasjon og lukkede forum. Stereotypien av en hacker er noe i retning av en ung, bleik mann, med kviser, joggebukse og Red Bull i neven. Var det slike vi ville finne – eller var det noe helt annet?

Som nevnt i innledningen til metoderapporten, hadde vi ingen ide om at vi i løpet av noen måneders jobbing - med løpende publisering – ville kunne hevde oss på hackernes egne jaktmarker på det mørke nettet. Hva kunne vi finne ut om dem, ved å bruke åpne kilder?

Killnet-angrepet aktualiserte dette: Var dette russiske agenter eller fjortiser på gutterommet? Eller begge deler? E-posten vi hadde avslørt, viste at det var kontakt mellom norske og russiske myndigheter tett opptil angrepet. Var Killnet-angrepet en politisk styrt aksjon? Hvordan kunne vi få tak i angriperne selv? Og hva kunne vi finne ut om dem?

2.8.1 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 hundrevis, og snart 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.

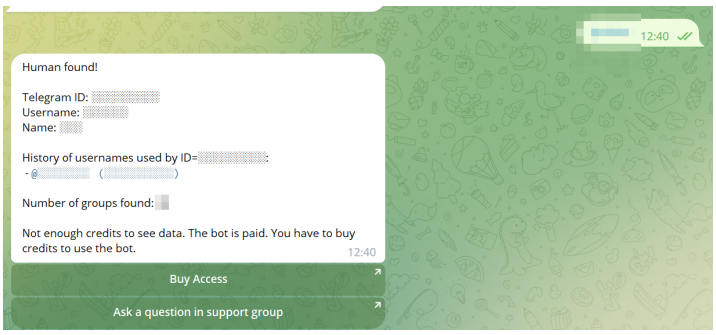
Samtidig var Killnet-angrepet en løpende nyhetshendelse der alle de store redaksjonene nå jobbet på høygir, så vi tok kontakt med kontoen – samtidig som vi researchet for å finne ut hvem det var.

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 – utover et slagord på latin.

Vi googlet brukernavnet, og fant at det var kontoer med samme brukernavn på flere andre sosiale medier. Flere av kontoene hadde samme navn og bilder som lignet - og indikerte at de tilhørte samme person. 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
Hvilke undersøkelser kunne vi gjøre i Telegram for å finne om Telegram-kontoen tilhørte personen vi hadde funnet i andre sosiale medier?

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.



TGSCANROBOT: Slik ser søkeresultatene ut i Telegram om du bruker TGScanrobot til å søke opp en konto.

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, sa han at navnet var riktig. Vi publiserte intervjuet med ham, der han sier at 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 oppsiktsvekkende påstand: Det skulle bli avholdt en «proukrainsk samling» på gressletta. Derfor måtte prorussiske aktivister samle seg og «mobilisere».

Vi reiste ut den aktuelle kvelden, da Killnet-aktivisten skulle mobilisere, men fant verken russere eller ukrainere. På gresset var det imidlertid tagget flere store Z-er – symbolet som indikerer støtte til Russlands invasjon av Ukraina – med teksten: «God morgen, Norge – hilsen Killnet». Med andre ord, hadde det faktisk vært en Killnet-tilknyttet person på norsk jord. Da vi oppdaget innlegget, saumfarte vi kommentarfeltet: Var det noen nordmenn der som ville slutte seg til markeringen?

2.8.2 Metode: Pimeyes

Innlegg fra en av personene som kommenterte, indikerte at vedkommende var norsk, eller i hvert fall oppholdt seg i Norge. Vedkommende var en kvinne, og det var flere bilder av henne på profilen.

Det er flere gode tjenester på nettet for omvendte bildesøk – Yandex, Google Images, Tineye og andre. Disse er gode til å søke opp bilder og omgivelser, men ikke optimalisert til å søke direkte på ansikter. Gravegruppa hadde på dette tidspunktet også et abonnement på tjenesten Pimeyes, som er et verktøy for å ansiktsgjenkjenning.

Vi søkte opp bildene av kvinnen i Pimeyes – og fikk 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. I intervjuet fortalte hun ikke bare om sin støtte til Killnet, men om grov hets hun fikk for sitt avvikende syn på invasjonen av Ukraina.

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 store angrep i Norge og skal ha forbindelser til russisk etterretning.

Fra en kilde som fulgte hackermiljøet tett fikk vi tips om en Twitter-konto som var svært interessant: Kontoen var anonym. Men den publiserte store mengder bilder, navn og informasjon på personer den hevdet var tilknyttet flere av de russiske hackergruppene – Conti, Revil, Killnet, Hive og andre. 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: Det var angivelige navn, bilder og en rekke personlige detaljer. Materialet som dukket opp i lekkasjene på Twitter-kontoen stammet eksempelvis fra at hackerne har brukt sine personlige e-postadresser 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 – på linje med det Dagbladet fant med Killnet-hackeren.

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 gjøre egne undersøkelser før vi – eventuelt - kunne publisere noe av det.

2.8.3 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 som postet informasjonen 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. Derimot skulle søkemotoren IntelX vise seg å bli veldig nyttig. IntelX går dypere, og søker ikke bare i nettsider – men finner informasjon på det mørke nettet, datalekkasjer og et utall åpne kilder. En viktig presisering er at IntelX ikke selv hacker eller bryter seg inn på nettsider. Men den fanger opp informasjon fra for eksempel 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.

2.8.4 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 derfor også opp bildene i bildegjenkjenningsmotoren Yandex. Den er russisk, men er fortsatt operativ tross invasjonen og krigføringen til Russland i Ukraina. Bellingcat er blant redaksjonene som anbefaler Yandex framfor Google Images og Tineye, og mener den gir bedre treffprosent. Spesielt gjelder dette østeuropeiske kilder – som var det vi søkte etter.

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 – med navnene Grønt, Gult og Rødt. Rødt var navnene der vi selv hadde funnet feil. Gult var navnene der vi var usikre. I den grønne mappa, lagde vi en liste over personer der følgende parametere var til stede.

- 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 personer som tilfredsstilte disse kravene, ble kontaktet for imøtegåelse – både direkte, og der det var mulig, via advokat. Det hele resulterte i saken «Serverte stjernene: - Var fryktet hacker»

2.9 Hvor kom pengene fra?

Det er ikke vanskelig å skjønne hvordan de såkalte «løsepengehackerne» - grupper som Conti, Revil, Evil Corp og Hive, tjener penger. Det gjør de ved gjennom selve hackereangrepene, der de infiserer datasystemer, stjeler informasjon og presser virksomhetene for penger etterpå. Med Killnet var det annerledes. Killnet-hackerne hadde tidligere drevet med løsepengeangrep og utvikling av skadelig programvare. Men etter invasjonen av Ukraina hadde gruppa relansert seg selv som en utelukkende politisk aktør, som deltok på lik linje med russisk etterretning i cyberkrigen mot Vesten, mot NATO og mot Ukraina. Denne virksomheten genererte ingen inntekter – i hvert fall så vidt vi kunne skjønne. Derfor stilte vi oss spørsmålet: Hvor får egentlig Killnet penger fra?

Donasjoner og sponsede innlegg
Vi fikk en del informasjon om finansieringen 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 erfaren eiendomsutvikler og boligmagnat 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, om hvorfor han kjøpte annonseplass hos en kjent hackergruppe. Galler sto som pålogget Telegram store deler av dagen, og meldingene våre ble raskt merket som «lest». Men vi fikk aldri noe svar.

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 framgikk det at selskapet var grunnlagt av Bakai Kolchaev – en kirgisisk gründer som hadde bygget opp et musikkimperium som var et av de mest betydningsfulle i den tidligere sovjet-republikken. Da vi tok kontakt reagerte Bakai Kolchaev sterkt på avsløringen. Han opplyste til oss at Infinity music fjernet Killnet-låta fra sine kanaler.

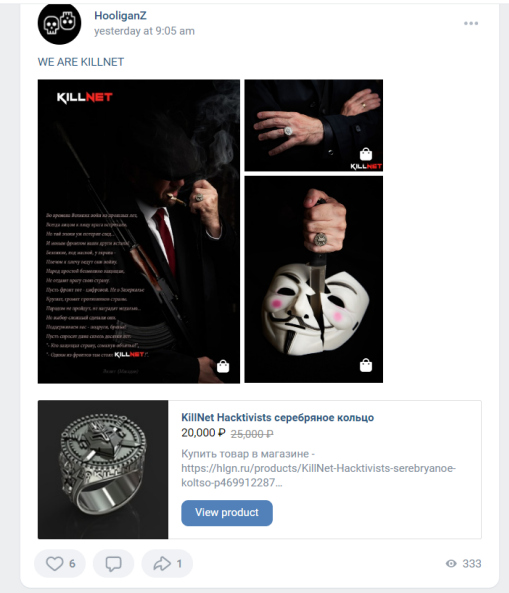
2.9.1 Metode: Selskapssøk i Russland og på Kypros

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?



STØTTET: Hooliganz prøvde ikke å skjule at de støttet hackerne i Killnet. Faksimile: VK

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: https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchResults.aspx?name=%25&number=401676&searchtype=optStartMatch&index=1&lang=EN&tname=%25&sc=1

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 selv – med sjefen i kopi – og ba om dokumentasjon for forbindelsene mellom Hooliganz Jewelry, ham selv og Killnet.

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. Til svar fikk vi nå en e-post fra sikkerhetssjefen i Exness, som kalte oss inn til et Google Meet-møte. Kort tid fikk vi en ny e-post fra sikkerhetssjefen.

> *«Hos Exness har vi nulltoleranse for alle skadelige eller hatefulle agendaer. Som en direkte konsekvens av sin tilhørighet til velkjente påvirkere, jobber ikke Roman hos oss lenger.»*

Roman Iuppa hadde fått sparken. Ermakov avsluttet:

> *«I suggest we cancel our meeting on Monday, as this concludes the matter for us. Thank you for bringing it to our attention.»*

Reportasjen fra Kypros heter: Hacker-pengene leder til ektepar

2.9.2 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 etter angrepet.

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 sendte informasjonen som Killnet-hackeren hadde delt med oss, til ulike kryptoeksperter - både i private kryptoselskaper og ved universiteter. Flere mente saken var interessant, men bemerket det samme vi

hadde tenkt: bitcoin er designet for ikke å være sporbart. Det var Colin Boyd, professor i informasjonssikkerhet ved NTNU, som snudde alt på hodet. Han bemerket:

> *«Her høres det nesten ut som de involverte* vil *bli sporet.*
> *For å bevise at en transaksjon fant sted.»*

Spørsmålene
Killnet-hackeren hadde delt tre transaksjoner med oss, som han jo inviterte oss til å grave i.

«Igor» oppga jo tre transaksjoner som han hevdet endte opp hos Killnet – 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 fått tilgang til fem konkrete bitcoin-adresser som alle, angivelig, kunne knyttes til Killnet. Vi måtte finne ut om «Igor» snakket sant – om transaksjonene han hadde sendt oss dokumentasjon på, virkelig endte opp hos Killnet. En god indikasjon på det, ville være om vi fant overføringer fra adressene som han hadde sendt oss – til adressene Killnet selv opererte med. Vi ønsket også å se hva vi kunne finne ut om Killnet sin økonomi, ved å granske overføringer fra bitcoin-adressene deres.

Bitcoin går i en endeløs sirkel fra konto til konto. Kunne vi finne ut hvor Killnets bitcoin stoppet? Kunne vi finne informasjon om aktører Killnet samarbeidet med?

Sporingen begynner
Så vidt vi kjente til hadde ingen norske journalister tidligere klart å spore bitcoin-transaksjoner på denne måten. Vi selv hadde definitivt ikke gjort det før. 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.
Når hver konto har relativt kronglete navn – et tilfeldig valgt eksempel:
bc1qng0keqn7cq6p8qdt4rjnzdxrygnzq7nd0pju8q – er det lett å gå seg vill.

Eksperten
Vi bestemte oss derfor for å finne en samarbeidspartner som kunne mer om dette enn oss. Når vi googlet norske kryptoeksperter var Torbjørn Bull Jenssen et navn som gikk igjen. Han er sjef i selskapet Arcane Crypto, og vi kontaktet ham og spurte om han kunne bistå oss i undersøkelsene. Han henviste til sin senioranalytiker Anders Helseth, som ble en nyttig sparringpartner.

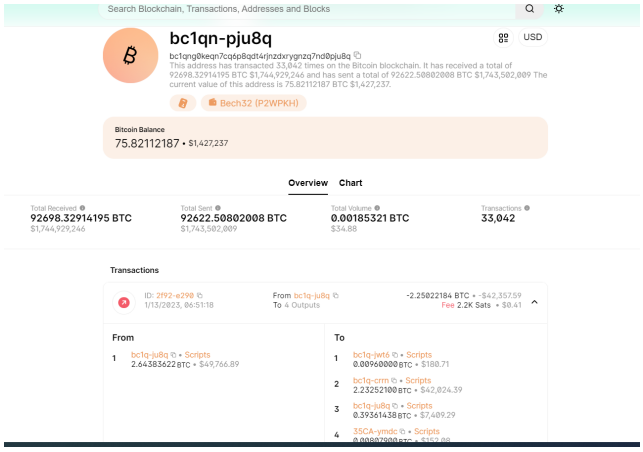
Hver konto har også et felt der det står «total received» - altså hvor mye bitcoin som totalt har gått inn på en adresse. Vi trodde først at dette kunne gi en indikasjon på hvor mye konto-eieren var god for. Der korrigerte Anders Helseth oss: det regnestykket ble for enkelt. Heller viste det hvor mye

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.

Funnene
Vi fulgte Killnets bitcoinoverføringer sammen med Helseth, og fant:

- 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 . Hvem sin milliard var det? Hadde Killnet *så* mye penger?



PENGESTRØMMEN: Slik ser siden til en vilkårlig valgt bitcoin-adresse ut på Blockchain.com. Øverst står kontonummeret, så står hvor mye penger som totalt har vært innom kontoen. Nederst står transaksjonene nedover – bildet viser den øverste transaksjonen. «From» er hvor pengene kom fra, «To» hvor pengene gikk videre.

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 forskningsrapporten, og i flere 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 «cold wallet» er et sikrere sted å ha pengene sine om de bare skal spares og ikke veksles ut – siden den ikke kan hackes. 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 sammen med Anders Helseth, viste at Killnet-pengene stoppet opp hos «hot wallet»-kontoen Bitfinex. Vi kunne ikke slå fast sikkert hva som skjedde med dem etterpå, men siden vi ikke fant at bitcoinene beveget seg videre er det ikke usannsynlig at de ble vekslet om 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. Vi har forsøkt å få dem til å utdype, men etter at bombardementet mot Kyiv ble gjenopptatt med angrep mot infrastruktur og strømkilder, har vi ikke fått flere svar.

2.9.3 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 såkalt Elon Musk-svindel – et nettfenomen 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 av dem.

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 på øya. Dermed kunne vi vise hvor lett det var å registrere selskap som i Norge ble brukt til kriminell virksomhet i saken: - Er det en bombe?

2.10 Hendrik Weber

Samtidig som vi begynte å undersøke hackerangrepene mot Norge, fikk vi et tips om en annen interessant forbindelse mellom Norge og Russland. Tipset gjaldt en profilert norsk lokalpolitiker – Hendrik Weber fra Rødt i Alver kommune. Weber var en kjent prorussisk stemme. Tipset lød på at han hadde bedre forbindelser i Russland enn tidligere kjent.

2.10.1 Metode: Russiske selskapssøk del 2

På Hendrik Webers nettside oppga han at han drev et selskap som het SRT24, at selskapet er registrert i Russland og at initialene står for «Scandinavian Russian Travel». Vi fant ett selskap med navnet SRT24 i selskapsregisteret på Rusprofile.ru. Selskapets daglige leder het Viktor Vasilievich.

Vi klikket på Vasilievichs navn, og oppdaget at han var involvert i en rekke andre virksomheter på den okkuperte Krim-halvøya. Det er ikke så mye informasjon tilgjengelig på gratisversjonen av nettsiden - men det var nok til at det vekket vår interesse. Blant annet registrerte han, seks uker før invasjonen av Ukraina, et selskap på Krim-halvøya som oppga at det skulle drive sykehus.

Dokumenter til Polen

Det var begrenset med informasjon tilgjengelig på gratisversjonen av nettsidene til Rusprofile. På nettstedet Info-Clipper kan du imidlertid bestille selskapsdokumenter fra bortimot hele verden. Vi søkte opp SRT24 og fant selskapet. Der kunne vi bestille en mer dyptgående selskapsrapport. Av grunner vi ikke kjenner til viste det seg at det ikke var mulig å bestille dokumenter med norsk betalingskort. Men vi hadde nylig vært på reportasjeturer til Polen for å dekke flyktningkrisa - og en polsk fotograf vi hadde samarbeidet med der, stilte opp og la ut med sitt polske kort.

I dokumentene fikk vi enda bedre oversikt over Viktor Vesna Vasilievich's virksomhet, og kunne slå fast at han var en nøkkelmann for Vladimir Putin på Krim. Han drev organisasjonen Union fra samme adresse som SRT24 i Moskva. På nettsiden til Union sto det oppført hvem som hadde tillitsverv i organisasjonen. Gjennom søk på russisk Google (Google.ru) og selskapssøk også på disse på Rusprofile, fant vi at flere av de involverte i Union var profilerte Putin-vennlige politikere. Union oppga selv å motta penger fra Dumaen i Moskva.

2.10.2 Metode: Innsyn i kommuneforslag

Vi ba også om innsyn hos Alver kommune, i de forslag Hendrik Weber hadde fremmet som kommunestyrerepresentant. I oversikten kommunen sendte tilbake, gikk det fram at han – til tross for at han satt i helsekomiteen i kommunestyret - hadde prøvde å stoppe NATO-ubåter med atomvåpen fra å bruke militærbasen Haakonsvern utenfor Bergen. Iver Neumann, direktør ved Fridtjof Nansens Institutt, menter Webers forslag var i Russlands interesse.

3 Spesielle erfaringer

3.1 Kontakten med Amedia

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, 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, slik vi beskriver i vår sak, 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 dette ikke er noe vi gjør i alle saker, og i hvert fall ikke i saker som angår konkurrerende mediehus. Derfor var vi tydelige på at dette forble mellom oss og ham.

«Når publiserer dere?» spurte Nedregotten oss, klokka 22.34 søndag 26. juni.

Vi svarte at publisering ble forsinket på grunn av terrorangrepet i Oslo, men at vi håpet på publisering i løpet av den kommende uka. Før vi hadde publisert, 28. juni, sendte Amedia ut pressemelding om hackerangrepet og om hvem som sto bak.

4 Sikkerhet og etikk

4.1 Sikkerhet

- All bruk av darkweb skjedde på en egen PC, som ikke var koblet på Aller-husets vanlige nett. På denne PCen lagret vi heller ingen annen informasjon, og logget ikke inn med våre brukerkontoer. 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 om nøyaktig hva andre hadde sagt, deres identitet eller opplysninger som kunne bidra til å identifisere dem. Vi antok at det kunne foreligge sikkerhetsrisiko for personer som var i kontakt med et vestlig medium.

4.2 Etikk

I vårt prosjekt befant en vesentlig del av kildene seg i Russland eller støttet Russland i krigen. Vi merket en kraftig skepsis fra flere – og møtte oss med svar som:

> *«Jeg vil først gjøre det klart hvilken type journalist du er. Tilhører du en fri presse, eller en presse som utvetydig er imot Russland?»*
>
> *«Du sier du er en undersøkende journalist. Gjøres dine undersøkelser på vegne av den norske stat, arbeider du for norske myndigheter?»*

Denne skepsisen og manglende tilliten fra mange russiske kilder utgjør et mulig presseetisk dilemma, da vi står fare for å miste en viktig stemme som kan balansere eller berike artiklene. Dette førte til at vi arbeidet ekstra hardt for å sørge for at kildene fikk oppfylt sin tilsvarsrett, og at de kunne ha tillit til at vi siterte dem korrekt. I de tilfellene kildene innledningsvis avviste å snakke med oss, gikk vi flere runder for å innhente kommentarer og tilsvar. Vi brukte også russiske tolker i enkelte intervjuer for at kildene skulle stole på at det de uttalte ble riktig forstått av oss. Vi ønsket de russiske kildene i tale – ikke minst for presseetikken og balansens del.

Et annet viktig perspektiv fikk vi med oss fra ofrene. 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 klare tilbakemeldinger på at dette hadde medført sikkerhetsrisikoer for dem – og at de ikke kom til å være så åpne neste gang. Det var et interessant og viktig perspektiv, som vi tok med oss når vi behandlet informasjon fra de andre ofrene. Vi unnlot eksempelvis å røpe for mange detaljer om hvordan hackere kom seg inn, hva som havnet på avveie og lignende.

5 Konsekvenser

Prosjektet «Sporene til Russland» har satt dagsorden og fått en rekke 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.

FIKK SPARKEN: - En russisk finansmann som sto bak et selskap som hjalp Killnet å tjene penger, fikk sparken fra jobben sin.

FJERNET RAP-LÅT: Den kjente russiske rapartisten Kaje Oboyma erklærte sin støtte i ei låt publisert sommeren 2022. Etter at vi kontaktet Oboymas distribusjonsselskap Infinity Music, tok de låta ned fra sine plattformer.

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.)

Sporene fra Hurtigruten

Politiet fant aldri ut hvem som hacket Hurtigruten i desember 2020. Nå kan Dagbladet avsløre hvem som sto bak - og deres linker til Vladimir Putins innerste krets.

DISSE HACKET

TEKST: TORGEIR P. KROKFJORD OG THOMAS FRIGÅRD
tpk@dagbladet.no

Det var natt til mandag 14. desember 2020 at Hurtigrutens datafolk oppdaget at noen var inne i datasystemene deres. Noen som hadde onde hensikter. Saken ble raskt meldt til politiet. Hurtigruten avdekket at angriperne fikk tak i personopplysninger tilhørende en rekke kunder.

En ting fant aldri politiet ut. Hvem sto egentlig bak angrepet?

– Saken ble henlagt i november 2021 på grunn av mangel på opplysninger om gjerningsperson, sier Asbjørn Bartnes, sjef for kommunikasjonsstaben i Troms politidistrikt, til Dagbladet.

– Hvordan ble saken etterforsket?

– Saken ble etterforsket og behandlet på ordinær måte, med en datateknisk etterforskning og andre undersøkelser, uten at man har klart å finne ut hvem som sto bak.

Dagbladet kan i dag avsløre at det var hackergruppa DoppelPaymer som angrep Hurtigruten.

Tok skylda

DoppelPaymer tok selv ansvar for angrepet på sin nå avstengte side på det mørke nettet, og deres rolle kommer fram i en kartlegging gjort med programvaren Dark Tracer, utviklet av det koreanske sikkerhetsselskapet NSHC. Programmet brukes til å kartlegge hackergruppene på det mørke nettet.

DoppelPaymers rolle bekreftes også av det norske IT-selskapet Atea, som er Hurtigrutens IT-leverandør. De sto selv oppført som et offer på DoppelPaymers side på det mørke nettet.

– Det var ikke Atea som ble rammet, men Hurtigruten, sier Thomas Tømmernes, IT-sikkerhetssjef i Atea til Dagbladet.

– Domenet deres, som vi drifter for dem, refererer til Atea. Det er bakgrunnen for at hackerne, Doppel-

MYSTERIUM: Vinteren 2020 var Hurtigruten gjenstand for et hackerangrep som kostet selskapet dyrt.

HURTIGRUTEN

Paymer, la ut Hurtigruten/Atea-domenet på sin side på det mørke nettet, sier Tømmernes.

Dagbladet har søkt DoppelPaymer på e-post - men den eneste kjente adressen deres er ikke lenger i bruk. Hurtigruten sier angrepet medførte en betydelig kostnad for selskapet. – Angrepet hadde en kostnad for Hurtigruten Group på rundt to millioner euro, hovedsakelig knyttet til å reinstallere servere og systemer som ble påvirket, sier kommunikasjonsrådgiver Tarjei Kramviken i Hurtigruten til Dagbladet.

Dødelig utfall

De første sporene etter DoppelPaymer dukket opp på det mørke nettet i april 2019. Gruppas mest alvorlige angrep fant sted 9. september 2020. Da slo gruppa til mot et universitetssykehus i den tyske storbyen Düsseldorf.

Da DoppelPaymer lammet sykehusets datasystemer, lå en kritisk skadd kvinne klar til å bli operert. Fordi datasystemet ble angrepet, kunne operasjonen ikke gjennomføres. Pasienten ble ifølge BBC lastet inn i en ambulanse, og i rasende fart fraktet til nærmeste nærliggende sykehus - i Wuppertal, tre mil unna.

Hun overlevde ikke den strabasiøse reisen.

Politiet etterforsket ikke lenger «bare» et dataangrep. Men også drap. Sporene ledet til Russland, opplyser det tyske IT-sikkerhetsdepartementet.

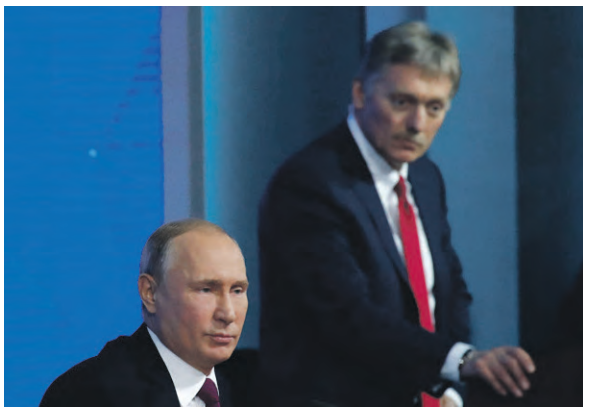
– Det som er kjent om angriperne bak DoppelPaymer indikerer at de bor i Russland, sier pressetalsperson Joachim Wagner til Dagbladet.

Forbindelsen

Vi kontakter den Canada-baserte IT-sikkerhetseksperten Brett Callow. Han har undersøkt programvaren, de tekniske løsningene, operasjonene og metodene til DoppelPaymer.

– Når du undersøker DoppelPaymer, og ser hvordan de har operert, leder alle spor til Evil Corp, sier Callow til Dagbladet.

→



TETT PÅ: Dmitry Peskov (t.h.) er president Vladimir Putins pressetalsperson og tett på den russiske presidenten. Peskov skal være en venn av Evil Corp-leder Maksim Yakubets. Foto: Reuters / NTB

Evil Corp er en av verdens mest kjente hackergrupper. Og har dokumenterte forbindelser både til russisk etterretning og Vladimir Putins indre sirkel.

– Det er definitivt bånd mellom DoppelPaymer og Evil Corp. De bruker en del felles tekniske løsninger, løsninger som ikke brukes av noen andre, sier Callow, som jobber i sikkerhetsselskapet Emsisoft.

– Både DoppelPaymer og Evil Corp har brukt spionprogramvaren Dridex, som igjen er utviklet av Evil Corp, sier Callow.

Evil Corp knyttes også til andre identiteter, som Indrik Spider og BitPaymer. Hvem er egentlig Evil Corp?

Vi går tilbake til 2019.

«Tyv»

Det var ikke vanskelig å legge merke til Maksim Yakubets, der han rånet rundt i sin kamuflasjelakkerte Lamborghini Aventador. Bilder offentliggjort av britisk politi, viser at Yakubets snakker med russisk trafikkpoliti. Og det er ikke vanskelig å skjønne at det var fristende å sjekke hva den tungt motoriserte italienske oksen var god for.

Kanskje bør du være ekstra varsom når bilskiltet ditt bærer ordet «BOP». «Tyv», på russisk. Ifølge FBI er Maksim Yakubets mannen bak pseudonymet «Aqua» på det mørke nettet, en av lederne i hackergruppa Evil Corp – og med det en av tidenes mest vellykkede nettkriminelle. Totalt skal Evil Corp ha tjent omkring 100 millioner dollar på sin kriminelle virksomhet.

FBI etterlyste i 2019 ni antatte medlemmer av hackergruppa med navn og bilde. BBC fikk tak i Maksim Yakubets' far i Moskva i november i fjor, men FBI er trolig maktesløse så lenge Yakubets oppholder seg i Russland. Han er en mann med gode kontakter.

Antatt spion

Yakubets er ifølge russiske medier en god venn av Dmitrij Peskov, Vladimir Putins pressetalsperson. Peskov har ikke besvart Dagbladets spørsmål til denne saken.

Det er også verdt å dvele litt ved Maksim Yakubets' overdådige bryllup, høsten 2019. Eduard Bendersky trakk ifølge Bellingcat i trådene da en tsjetsjensk militærleder ble drept - av en russisk etterretningsoffiser - midt i en park i Berlin i 2019.

Mens Eduard Bendersky planla likvidasjonen på tysk jord, mener USA at også svigersønnen jobbet for etterretningstjenesten FSB, samtidig som han var en av verdens farligste hackere. Da Maksim Yakubets ble etterlyst av FBI, offentliggjorde USA at de mener EvilCorp-lederen hadde jobbet for russisk etterretning siden 2017.

Hurtigruten ønsker ikke å kommentere at de ble angrepet av hackere med linker til russiske myndigheter. Kommunikasjonsrådgiver Tarjei Kramviken sier:

– Vi ønsker ikke å bidra til økt oppmerksomhet rundt slike kriminelle grupper, siden det tjener deres sak når metoden er å utpresse ofrene ved å true med publisering av stjålet materiale. Økt oppmerksomhet vil kunne gjøre den typen utpressing mer effektiv. Vi har ikke kompetanse til å vurdere hvem personene som står bak er og hvilke relasjoner de har til andre, det er det best at eksperter på IT-sikkerhet eller myndighetene gjør.

Etterretningskobling

En slik er Jørgen Rørvik, direktør for cybersikkerhet i IT-giganten Sopra Steria.

– I september 2021 publiserte det kjente cybersikkerhetsselskapet Recorded Future en rapport som redegjorde for både direkte og indirekte koblinger mellom Russland og cyberkriminelle, sier Rørvik til Dagbladet.

FLASHY: Maskim Yakubets med en russisk politimann, og sin kamuflasjekledte Lamborghini. Foto: National Crime Agency

STABLER MED CASH: Et antatt Evil Corp-medlem poserer med en pengestabel på et bilde offentliggjort av britisk politi. Foto: National Crime Agency

OVERDÅDIG: Det ble ikke spart på noe da Maksim Yakubets giftet seg med datteren til en betrodd offiser i den russiske etterretningstjenesten FSB. Foto: Skjermdump

Han understreker at han ikke kjenner angrepet mot Hurtigruten i detalj. Men på generell basis er også han kjent med koblingene mellom Evil Corp og russiske myndigheter.

– Ifølge Recorded Future er det meget sannsynlig at russisk etterretning har et forhold til cyberkriminelle, i særdeleshet gruppen «Evil Corp», sier Rørvik.

– Utfordringene dette skaper er uklare linjer mellom hva som oppfattes som kriminelle handlinger motivert av økonomisk vinning og hva som betraktes som spionasje og destruktive operasjoner. Forholdet bidrar også til at kriminelle grupper har tilgang på særdeles avanserte virkemidler for å oppnå sin målsetning, som i sin tur kan være i tråd med russiske interesser.

To millioner euro

Ifølge advokatfirmaet Clyde & Co, som med hovedkontor i London har en rekke klienter innen shipping- og cruisebransjen, er DoppelPaymer en av to hackergrupper som har spesialisert seg nettopp på selskap innen maritim sektor. Den andre heter WastedLocker, og ifølge den anerkjente cyberanalytikeren Pieter Arntz er det EvilCorp som står bak også den.

Ifølge Clyde & Co. skal DoppelPaymer og WastedLocker ha tjent over 50 millioner dollar i kryptovaluta. Kommunikasjonsrådgiver Tarjei Kramviken sier Hurtigruten ikke vet hvor mye DoppelPaymer krevde i løsepenger.

– Vi gikk aldri i dialog med utpresserne. Vi hadde tidlig kontakt med politiet og hadde full åpenhet med dem rundt situasjonen. Vi kjenner ikke til hvilke krav eller lignende som kan ha blitt stilt ettersom vi ikke hadde noen dialog med angriperne. Vi opprettholdt driften på skipene som var i trafikk, med manuelle løsninger. Vi benyttet sikkerhetskopier og rutiner for gjenoppretting til å reetablere IT-systemene våre.

Nytt navn

Hackerne som angrep Hurtigruten, er fortsatt aktive. Men ifølge flere analytikere har DoppelPaymer nå skiftet navn, og endret framtoningen sin på nett – til å nå operere under navnet Grief: «sorg» på norsk. Gruppa har også sluttet å kreve løsepenger i Bitcoin – og foretrekker i stedet at ofrene betaler dem i en kryptovaluta som har en spesiell klang i Norge: Monero.

Det er den samme kryptovalutaen som Tom Hagen, Anne Elisabeth Hagens drapssiktede ektemann, hevder han ble bedt om å betale løsepenger i for å få kona si tilbake.

– Vi ser at det skjer flere og flere transaksjoner i Monero, sier Brett Callow.

– Er Monero vanskeligere å spore enn Bitcoin?

– I teorien er den i hvert fall det.

Denne artikkelen er laget i et samarbeid mellom Dagbladet og Kommunal Rapport.

MILLIONSMELL: Hurtigruten - her ved direktør Daniel Skjeldam - oppgir at dataangrepet kostet dem to millioner euro. Foto: NTB

SIKKERHETSEKSPERT: Jørgen Rørvik er direktør for cybersikkerhet i Sopra Steria. Foto: Sopra Steria

BLANK SIDE

HACKER-ANGREPET

HACKERE ANGREP NORGES HJERTE

UTENRIKSMINISTERENS BILDE MISBRUKT: Den russiske hackergruppen Killnet har publisert dette manipulerte bildet av Norges utenriksminister Anniken Huitfeldt på Telegram. Skjermdump hentet fra Telegram. Foto: Beate Oma Dahle / NTB

Russiske hackere angrep i går flere av Norges viktigste samfunnsorganer. Nato-sjef Jens Stoltenberg er blant dem som har fått trusler.

God morgen Norge! Alle lag til angrep! Slik startet den russiske hackergruppa Killnet gårsdagen.

Få timer seinere hadde de lyktes med å ta ned eller destabilisere en rekke nettsider til store norske offentlige virksomheter.

Både BankIDs nettsider og Arbeidstilsynets nettsider var nede, og Altinn skrev at «enkelte brukere opplever ustabilitet».

Det var Dagbladet som tidlig på formiddagen avslørte angrepet fra Killnet.

«Mrs. Error»

Hacker-gruppa er en kjent prorussisk aktør, som har stått bak en rekke dataangrep til støtte for invasjonen av Ukraina.

På det sosiale mediet Telegram la gruppa ut et bilde av utenriksminister Anniken Huitfeldt med det som ser ut som en Maleficent-maske, fra Disney-filmen med samme navn, kunne Dagbladet fortelle.

«Mrs. Error», kaller gruppa Norges utenriksminister.

Gruppa hevdet å planlegge angrep på politiet, BankID, ID-porten hos Difi, Nav, UDI, Digitaliseringsdirektoratet og flere andre norske nettsider og nettjenester.

– Spør Biden

I et eksklusivt intervju med Dagbladet onsdag ettermiddag, kom en person tilknyttet gruppa via en Telegram-konto med følgende advarsel

– Ikke rør Russland!

På spørsmål om bakgrunnen for angrepet svarte han:

– Spør Biden. (...) Dere har blokkert mattilgangen til våre innbyggere. Dette er den russisk-norske grensa – I hvert fall burde det være det.

Killnet offentliggjorde tidligere onsdag at årsaken til det massive angrepet mot norske nettsider var at Norge ikke tillater frakt av russiske varer til gruvebyen Barentsburg på Svalbard via Storskog.

«Jens fiende nr. 1»

Killnet har stått bak en rekke dataangrep til støtte for invasjonen av Ukraina. Tidligere i sommer skrev gruppa:

«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.»

Gruppa hevder på Telegram å ha en kopi av Jens Stoltenbergs pass. Det har de ikke, viser Dagbladets undersøkelser.

Personnummeret matcher ikke Stoltenbergs oppføring i Folkeregisteret pr. nå. Bildet er også hentet fra en annen nettside. På spørsmål fra Dagbladet bekrefter også en talsperson for Nato:

– Vi kommenterer ikke sikkerhetssituasjonen rundt generalsekretæren. Bildet du har sendt oss er også falskt, og ikke et bilde av generalsekretærens pass.

– Under kontroll

Blant dem som fikk merke angrepene utover dagen i går, var avisa VG.

– Vi jobber på spreng for å finne ut av dette. Vi beklager ulempene dette medfører til alle våre brukere, sa utviklingsredaktør i VG Øyvind Brenne til sin egen avis.

– At Norge nå har opplevd et cyberangrep, er en del av det vi nå må være forberedt på, sa stats-

– MÅ VÆRE FORBEREDT: Statsminister Jonas Gahr Støre, på Nato-toppmøtet Summit2022 i går. Foto: Bjørn Langsem

FALSKE PASS-PÅSTANDER: Hackergruppa Killnet hevder å ha en kopi av Jens Stoltenbergs pass. Det har de ikke, viser Dagbladets undersøkelser. Her er Stoltenberg på gårsdagens Nato-toppmøte. Foto: NTB /AP/Susan Walsh

«GOD MORGEN NORGE! ALLE LAG TIL ANGREP!»

MELDINGA FRA HACKERGRUPPA

minister Jonas Gahr Støre (Ap) da han møtte pressen ved 14.40-tiden.

Han understreket samtidig at situasjonen med hackerangrep mot flere norske sider da var under kontroll, og at angrepet så langt ikke hadde fått alvorlige følger.

– Startet klokka 02

Ifølge Altinns pressesjef startet angrepet rundt klokka 02 natt til onsdag.

– Vi kan bekrefte at det har pågått et tjenestenektangrep mot Altinn og Id-porten. Det startet cirka klokka 2 natt til onsdag, sa kommunikasjonsansvarlig Jørgen Ferkingstad til TV 2.

Han sa at det dreier seg om et tjenestenektangrep, altså et såkalt DDoS-angrep. Det betyr at noen forsøker å overbelaste serverne til nettsidene.

– Tjenesten er oppe igjen, men vi har satt inn begrensninger på antall brukere for å forhindre angrepet. Det fører til at noen enkelte, vanlige brukere vil oppleve ustabilitet ved bruk av tjenestene, men den vil nå fungere for de aller fleste, sa Ferkingstad.

«Kriminell prorussisk gruppe»

– Angrepene er rettet mot en rekke store norske virksomheter som tilbyr viktige tjenester til befolkningen, sa direktør for Nasjonal sikkerhetsmyndighet (NSM) Sofie Nystrøm i en pressemelding.

Hun bekreftet at en «kriminell prorussisk gruppering» virker å stå bak angrepene.

– Vi har sett liknende angrep i andre land den siste tiden, men ingen av disse har meldt om varige konsekvenser. Angrepene vil likevel kunne skape usikkerhet i befolkningen, og gi inntrykk av at vi er en brikke i den pågående politiske situasjonen i Europa, skriver Nystrøm.

– Sverget troskap til Putin

Dagbladet har vært i kontakt med Sissel Kruse Larsen, kommunikasjonsrådgiver for Natos generalsekretær, som henviser til Nato sentralt.

Dagbladet har også kontaktet arbeidsgiver og agent til Stoltenbergs barn. Stoltenbergs kone Ingrid Schulerud ønsker ikke å kommentere saken.

Det amerikanske føderale datasikkerhetsorganet Cybersecurity and Infrastructure Security Agency (CISA) la 20. april i år ut en rapport der de viste til at flere hackergrupper har sverget troskap til den russiske regjeringen og/eller det russiske folk, og at disse gruppene har truet med hevnaksjoner for angrep mot Russland eller støtte til Ukraina.

PST på saken

Mens store deler av staben i Politiets sikkerhetstjeneste, nærmest har jobbet døgnet rundt med terrorangrepet de siste dagene, måtte PST i dag sette store ressurser på det russiske hackerangrepet mot Norge.

– Vi er godt kjent med angrepet, og jobber med det, er det eneste kommunikasjonsrådgiver Annett Aamodt i PST vil si til Dagbladet om hackerangrepet.

Hun ønsker ikke å gi flere detaljer enn at PST er kjent med angrepet.

REPORTASJE

TORGEIR P. KROKFJORD
tpk@db.no
THOMAS FRIGÅRD (KOMMUNAL RAPPORT)
OLA STRØMMAN
olast@db.no
SIRI ÅBØ WIERSEN
siri.wiersen@db.no
BRAGE LIE JOR
brage.jor@db.no
EMMA SOFIE SØRLI
emma.sorli@db.no

HACKER-ANGREPET

DETTE KAN VÆRE KONSEKVENSENE

VIL RAMME SAMFUNNET: Den russiske hackergruppen slo til mot offentlige tjenestesteder. Målet er å lamme samfunnsviktige funksjoner som betalingstjenester, service og kommunikasjoner. Foto: NTB

Ole Tom Seierstad, sikkerhetssjef i Microsoft, forteller til Dagbladet at hvilke konsekvenser slike angrep kan få, avhenger av flere faktorer.

Han understreker at han uttaler seg på generelt grunnlag.

– Et typisk angrep for å ta ut sider, er DDOS-angrep, denial of service, også kalt tjenestenektangrep. Det betyr at man rett og slett styrer masse trafikk til enkelte sider, slik at de ikke klarer å holde unna trafikken, og krasjer. Det kan være snakk om hundretusener i sekundet, istedenfor tusener, som kanskje er designet.

– Straks mer alvorlig

I går var BankID ute av drift, det samme med sidene til Arbeidstilsynet.

«FORDI DET SOM OFTE SKJER, ER AT ANDRE HACKERMILJØER FØLGER OPP I STØYEN SOM NÅ OPPSTÅR.»
THOMAS TOMMERNES, sikkerhetssjef i Atea

– Bank ID er jo en tjeneste som mange andre tjenester er avhengige av, som offentlig sektor, banker, og slike ting. Er det et tjenestenektangrep, så er det egentlig bare støy og forstyrrelse av daglig drift, og ingen data på avveie.

Sikkerhetssjef Thomas Tommernes i Atea sier til Dagbladet at Killnet trolig har screenet nettsider i forkant av angrepet, og identifisert mål det er mulig å ta ut.

Han mener det trolig er snakk om nettopp et DDOS-angrep – altså at det påføres så mye støy på nettsida at den til slutt ikke klarer å svare.

Hackermiljøer kan følge opp

Tommernes sier at disse nettsidene dermed ikke er hacket i betydning at noen har kommet seg inn i systemene.

– Betyr det at det er begrenset skadepotensial?

– Det er vanskelig å svare på. Fordi det som ofte skjer, er at andre hackermiljøer følger opp i støyen som nå oppstår. Så når alle nå blir opptatt med å beskytte hoveddøra, kan noen ta seg inn gjennom kjellervinduet.

Er det derimot slik at hackerne har kommet seg inn i systemet, og ikke et angrep som har styrt trafikk mot nettstedene, er det straks mer alvorlig, sier Microsofts Seierstad.

– Da er det en risiko for manipulering av data, falske nyheter, og tyveri av opplysninger.

– Det tredje alternativet, som er enda verre, er om hackerne slipper ut et krypteringsvirus når de er inne i systemene. Det har man blant annet sett i Ukraina, hvor det ble sluppet ut et slikt virus mot sentrale myndigheter. Da blir alle data kryptert, uten mulighet for å få de tilbake, dersom det ikke er tatt back up. Det er virkelig alvorlig, sier han.

Statssponsede angrep

Seierstad i Microsoft sier det er sett et høyt aktivitetsnivå mot Norge fra Russland den siste tida. Spesielt mot nordområdene og Nato. Siste halvår i fjor lå Norge forholdsvis høyt på angrepslista, sett i forhold til størrelse på landet.

Seierstad har ingen informasjon om gruppa Killnet, men sier hackerangrep kan komme fra både enkeltstående grupper og være fra en nasjonalstat. Sistnevnte betyr at det ikke er svindlere eller kriminelle som står bak, men at det er snakk om statssponsede angrep.

– Vi ser dem spesielt fra Kina, Nord-Korea, Iran, og Russland. De har vært spesielt aktive fra siste halvår i fjor, sier Seierstad.

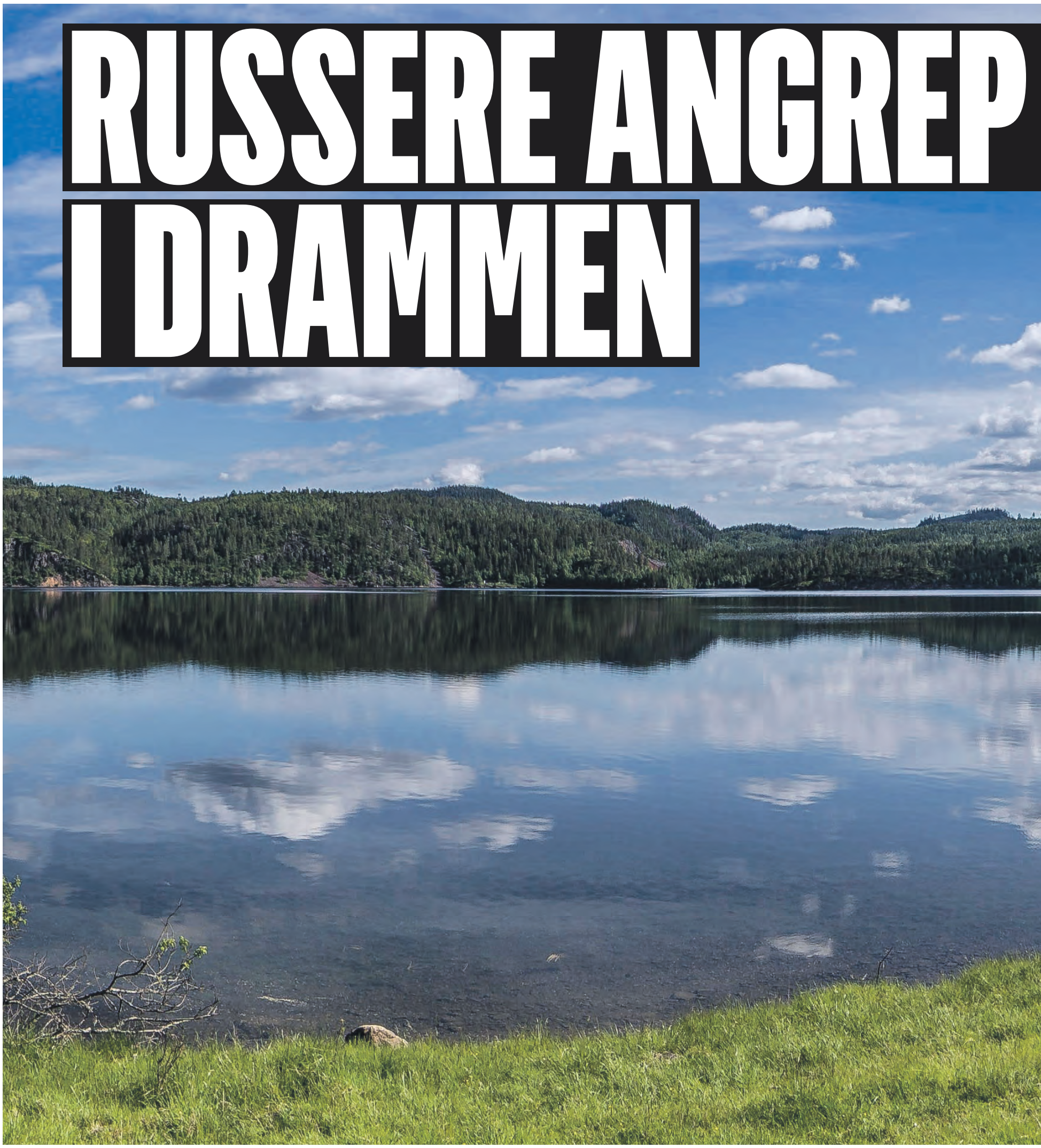
Hos Microsoft holder de nå øye med 150 ulike statssponsede hackergrupper, og kan kjenne dem igjen på blant annet mønster og metode, forteller han.

REPORTASJE
MARTHE SMÅKASIN LIEN
hanne.lien@db.no
JON EVEN ANDERSEN
jea@db.no
TORGEIR P. KROKFJORD
tpk@db.no
OLA STRØMMAN
olast@db.no
NIKOLAI ERIKSEN
nicolai.eriksen@db.no

BLANK SIDE

ANGREP VANNSYSTMET

RUSSERE ANGREP I DRAMMEN



THOMAS FRIGÅRD
Kommunal Rapport
TORGEIR P. KROKFJORD
tpk@dagbladet.no

Russiske hackere rystet Norge i slutten av juni, da de lammet en rekke offentlige nettsteder i et varslet angrep. Hackerne var i intervju med Dagbladet åpne på at angrepet var politisk motivert.

Tidligere har Dagbladet avslørt at russiske hackere også angrep Hurtigruten og Amedia – to store dataangrep der angriperne tidligere ikke har vært kjent.

I midten av februar i fjor ble Drammen kommune utsatt for et hackerangrep på en del av infrastrukturen for vann og avløp. Dagbladet og Kommunal rapport kan nå avsløre at hendelsen ble satt i sammenheng med et forsøk på å forgifte drikkevann i et område i Florida.

Angrepet skjedde nemlig kort tid etter at et vannverket i Oldsmar i Florida i USA ble utsatt for et datainnbrudd.

– Hendelsen i USA var interessant, siden det var et lite vannverk. Vi tok da en vurdering av datasikkerheten i vannverk, og konklusjonen er egentlig ikke overraskende, sier daglig leder Margrete Raaum i cyberresponsselskapet KraftCERT.

Dagbladet AVSLØRER Dagbladet

– Justerte opp giftige stoffer

I Florida klarte hackerne å koble seg inn på skalasystemet til vannforsyningen til 15 000 innbyggere, og de justerte opp mengden av det giftige stoffet lut i vannet til over 100 ganger normalnivået. Lut benyttes til å justere pH-verdiene i vannet.

Dette kunne ha gitt konsumentene etseskader på hud og slimhinner, i verste fall fatale følger.

Ifølge CNN er det uklart hva slags konsekvenser det ville ha fått om hackingen i Florida ikke hadde blitt oppdaget raskt.

– Kunne skjedd i Norge

Hendelsen førte til at alarmen gikk i cyberresponsmiljøet i Norge. Datasikkerhetsspesialistene i kommunesektoren, kraft- og petroleumsbransjen, og vannbransjen vurderte om tilsvarende hendelse kunne ha skjedd i Norge. De utformet et etterretningsnotat som ble sendt ut til norske kommuner med en tydelig konklusjon.

VANNSYSTEMET

Kort tid etter at hackere forsøkte å forgifte drikkevannet til 15 000 i USA, brøt russiske hackere seg inn på vannsystemet til Drammen kommune. Da gikk alarmen.

DRIKKEVANNSKILDEN GLITRE: Russiske hackere angrep vannsystemet i Drammen kommune. Her er drikkevannskilden Glitre utenfor Drammen.
Foto: Per Fjordvang

«Tilsvarende sikkerhetsmangler vet vi at også finnes i Norge. Om ikke disse håndteres vil tilsvarende angrep sannsynligvis gjennomføres mot norske virksomheter», heter det i etterretningsnotatet utformet av KraftCert, Kommune-CSIRT og Norsk Vann.

– Aldri noen fare

I brevet til kommunene ble angrepet mot Drammen kommune betegnet som «en pågående sikkerhetshendelse hos en norsk kommune», og kommunene ble oppfordret til å gjennomgå datasikkerheten på vann- og avløpssystemet.

– I Florida var det snakk om helt elementære brudd på sikkerheten, og vi er noe bedre rustet i Norge. Men, det er gjerne snakk om eldre systemer i vann- og avløpsetatene, og dette medfører større sårbarhet og større beskyttelsesbehov, sier Raaum.

Ifølge Drammen kommune skjedde datainnbruddet på en server uten kontakt med selve vannforsyningssystemet.

– Det var aldri noen fare for at dette dataangrepet truet vannforsyningen på noen måte, og hackerne fikk heller ikke tilgang på personinformasjon. Det var ingen stor trussel, men det skulle aldri ha skjedd, sier virksomhetsleder IKT Svein Hilding Aasen i Drammen kommune.

Kommunen engasjerte Atea IRT for å undersøke datainnbruddet, og selskapet har utformet en rapport om hendelsen. Drammen kommune har nektet Dagbladet og Kommunal Rapport innsyn i rapporten.

Russiske aktører

Dagbladet og Kommunal Rapport kan avsløre at det var den russiske hackergruppen Avaddon som sto bak dataangrepet mot vanninfrastrukturen i Drammen. Dette bekreftes også av kilder i Drammen kommune.

Ifølge teknologinettstedet zdnet.com la hackergruppen Avaddon ned sin virksomhet i juni 2021, noen måneder etter angrepet mot Drammen.

Kommunal Rapport og Dagbladet har forsøkt å spore opp medlemmer av Avaddon for å kommentere saken, men vi har ikke lykkes å komme i kontakt med gruppen.

– Typisk løsepengeangrep

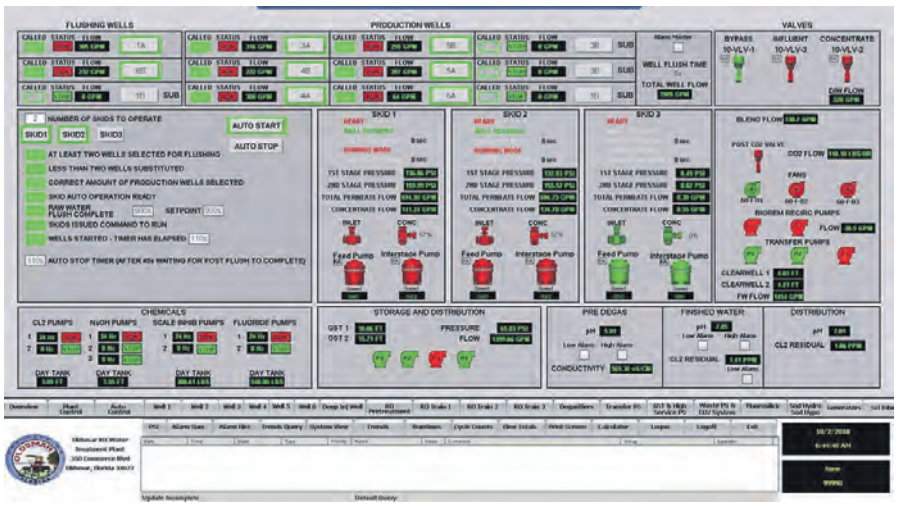
Hackerne krypterte filene på en server driftet av vann – og avløpsetaten, men gode back up – rutiner sørget for at kom-

➜ FORTS. NESTE SIDE

ANGREP VANNSYSTEMET

SIKKERHETSMANGLER: Margrete Raaum er daglig leder for datasikkerhetsselskapet KraftCERT. I et notat peker selskapet på at det finnes sikkerhetsmangler ved norske vannverk. Foto: KraftCERT

IKKE BEKYMRET: Avdelingsleder Kjetil Furuberg i Norsk Vann er ikke bekymret for at innbyggerne skal få helseskadelig vann grunnet dataangrep. Foto: Norsk Vann



KONTROLLSYSTEMET: Dette er kontrollsystemet til vannverket i Oldsmar i Florida. En hacker brøt seg inn på systemet og justerte opp lutnivået i vannet 100 ganger. Feilen ble raskt oppdaget av en våken ansatt. Foto: Privat

ADVARER: Bjørn Tveiten i KommuneCSIRT advarer om datasikkerheten i vann- og avløpssystemene i kommunene. – Vann og avløp er en kritisk tjeneste, påpeker han. Foto: Kristian Ridder-Nielsen

ANGREPET FØRST: Det alvorlige datainnbruddet på vannforsyningssystemet i Oldsmar i Florida kunne ha skjedd i Norge, mener norske cyberspesialister. Foto: Google Maps

«DET ER GJERNE SNAKK OM ELDRE SYSTEMER I VANN- OG AVLØPSETATENE, OG DETTE MEDFØRER STØRRE SÅRBARHET OG STØRRE BESKYTTELSESBEHOV.»

MARGRETE RAAUM, daglig leder i cyberresponsselskapet KraftCERT

➜ FORTS. FRA FORRIGE SIDE

munens data var sikret. Politiet mener at alt tyder på at det var et typisk løsepengeangrep.

– Vi har konkludert med at hensikten bak dataangrepet var økonomisk vinning, og ikke terror eller skade. Etterforskningen klarte ikke å identifisere angripernes IP-adresse, og saken er derfor henlagt grunnet ukjent gjerningsperson, sier politiinspektør Hans Erik Seljordslia i politidistriktet Sør-Øst.

Han ønsker ikke å kommentere opplysningene Kommunal Rapport og Dagbladet sitter på om at det var hackergruppen Avaddon som sto bak angrepet.

– Urovekkende

Undersøkelser fra Dagbladet og Kommunal Rapport viser at en rekke kommuner, fylkeskommuner og statlige etater har blitt utsatt for datainnbrudd de siste åra, og mange av angrepene er utført av russiske hackergrupper. Angrepet på Østre Toten i september i fjor er et eksempel på dette.

Cyberspesialistene i Kommune-CSIRT mener det er sikkerhetshull i kommunenes systemer for vann- og avløp.

– Vi ser at datasikkerheten i kommunenes VA-systemer ofte er hakket lavere enn det vi ser på IKT-systemene generelt. Det er urovekkende, og jeg frykter at det som skjedde i Florida også kan skje i Norge, sier leder av Kommune-CSIRT Bjørn Tveiten.

FAKTA

KOMMUNE-CSIRT OG KRAFTCERT

- Kommune-CSIRT er et nasjonalt senter for kommuner og fylkeskommuner for å informere og styrke cybersikkerheten.
- Senteret ble opprettet i 2020, og en av senterets oppgaver er styrking av datasikkerheten i vann og avløpssektoren.
- Senteret deltar i sektornettverket til Nasjonal sikkerhetsmyndighet (NSM). Det er et IKS eid av Gjøvik og Lillehammer kommune
- Rundt 50 av 356 norske kommuner er medlemmer av senteret.
- KraftCERT er et cyberresponsmiljø for sektorene kraft og petroleum, og ellers består målgruppen av prosessindustri, vann- og avløpssektoren samt energigjenvinning.
- KraftCERT samarbeider med Norges vassdrags- og energidirektorat (NVE) Petroleumstilsynet (Ptil) og Nasjonal sikkerhetsmyndighet (NSM)

KommuneCSIRT mener at digitaliseringen av vann og avløpssystemet og IKT-tjenestene har skjedd uavhengig av hverandre i de fleste kommuner. Dette fører til datastrukturen i vann – og avløpssektoren ikke nødvendigvis får like høy datasikkerhet som IKT-tjenestene.

– Hovedårsaken til denne skjevheten i datasikkerhet kan ligge i at ansatte i vann- og avløpsetatene, naturlig nok, ikke har den samme kompetansen på datasikkerhet som fagpersonene i IKT-avdelingene, sier Tveiten.

Lavere sikkerhet

– Burde ikke datasystemene for vann hatt ekstra høy sikkerhet?

– Jo, dette er en svært kritisk tjeneste, og vi er veldig engstelige for sårbarheten til vann- og avløpsstrukturen når det gjelder datasikkerhet. Dette er et område vi mener kommunene raskt bør ta tak for å øke sikkerheten, sier Tveiten.

Som i mange andre kommuner hadde vann- og avløpsetaten i Drammen egne servere for vann og avløpssystemet. Denne serverparken ble driftet av VA-etaten alene. Etter dataangrepet har kommunen endret strategi for å styrke datasikkerheten for VA-systemet.

– Nå har vi en felles strategi, og det er en stor fordel. Å ha en profesjonell IKT-organisasjon i ryggen gir helt klart en ekstra trygghet, sier Aasen i Drammen kommune.

- Kan skape krøll og støy

Norsk Vann er den nasjonale interesseorganisasjonen for vannbransjen. Organisasjonen eies av kommunene, og totalt er 320 av landets 356 kommuner medlemmer. Organisasjonen viser til sikkerheten for infrastrukturen for vann er høyt prioritert av kommunene, og at det skal mye til for at hackere skal ta kontroll over driftskontrollsystemet for vann.

– Hacking kan skape masse krøll og støy, og det kan muligens medføre mindre forstyrrelser i vannleveransene, sier avdelingsleder Kjetil Furuberg for vanntjenester i Norsk Vann. At det er svakere datasikkerhet i VA-sektoren enn i IKT-sektoren mener han ikke er et gitt faktum i alle kommuner.

– Dersom det mangler riktig og tilstrekkelig datakompetanse i VA-avdelingene er det rimelig å anta at datasikkerheten er lavere for VA enn for IKT, sier Furuberg.

Men det er vanskelig å si noe konkret om dette, sier Furuberg.

Han peker på at infrastrukturen for vann er nøye overvåket, og at det i kritiske situasjoner er mulig å løse eventuelle utfordringer manuelt, eller ved å benytte reservevannsforsyning.

– Er ikke så bekymret

– Det er mulig hackere kan forstyrre vannleveranse og svekke rensingen av vannet i en kortere periode, men jeg er ikke så bekymret for at innbyggerne skal få helseskadelig vann som følge av datainnbrudd, sier han.

Han viser til at kommunene må ha et bevisst forhold til trusselbildet, og at IKT-tjenesten og vann- og avløpstjenesten må samarbeide.

Han tror at de mellomstore kommunene kan ha vanskeligheter med å sikre seg nok kompetanse innen datasikkerhet på vann- og avløpsområdet.

● *Denne artikkelen er laget i et samarbeid mellom Dagbladet og Kommunal Rapport.*

BLANK SIDE

SPORENE TIL RUSSLAND

KREVENDE: – Hackingen gikk på psyken løs, sier Gjermund Tolpinrud i Sullestad.

SPORENE TIL RUSSLAND

DA HACKERNE SLO TIL: – FIKK HELT NOIA

På tre år har nesten 50 norske bedrifter og kommuner blitt utsatt for datainnbrudd av russiske hackerbander. Ofrene opplever angrepene som et helvete.

SPORENE TIL RUSSLAND

FORTVILET: Hele datasystemet til renholdsfirmaet Sullestad ble lammet av russiske hackere, sier daglig leder Gjermund Tolpinrud.

TOTEN (Dagbladet:)

Det er en helt vanlig arbeidsdag. Du skal bare sende en e-post før du tar helga. Plutselig starter dataskjermen å flimre. Så blir teksten på alle åpne program fullstendig uleselig. Lettere irritert forsøker du å åpne et nytt program.

Da dukker det opp en tekstboks du aldri har sett maken til.

«Velkommen. Hva har skjedd? Alle dine datafiler har blitt kryptert og er for øyeblikket utilgjengelig. Alt er mulig å gjenopprette, men da må du følge våre instruksjoner. Hvis ikke, vil du aldri få tilbake dine data».

For å kunne frigi tapt data får du beskjed om å kjøpe kryptovaluta – Bitcoin eller Monero – for et gitt millionbeløp.

Du har nettopp mistet kontrollen over bedriften din.

KAOSET HAR STARTET.

– Hele bedriften ble fullstendig satt ut av spill, sier daglig leder Gjermund Tolpinrud i renholdsselskapet Sullestad Support AS på Toten.

– Vi mistet alt vi hadde lagret av datafiler. Vi startet helt på null igjen. Det unner jeg ingen å oppleve, sier Raymond Elde i Radio Nordkapp – selvtitulert kringkastingssjef.

De to er blant de omkring 50 norske virksomhetene som er blitt angrepet av hackere de siste tre åra. Dagbladet og Kommunal Rapport har undersøkt angrepene, og finner at majoriteten av angrepene er utført av hackergrupper med forbindelser til Russland.

Hackerne ser ikke ut til å bare sikte seg inn på selskaper med store pengesekker.

De leter også etter de enkle byttene.

«Jeg møtte en blå skjerm, og en beskjed om at alle våre data hadde blitt kryptert. Selv om jeg var forberedt, fikk jeg helt noia.»

GJERMUND TOLPINRUND, daglig leder i renholdsselskapet Sullestad Support AS

FIKK HELT NOIA

I idylliske omgivelser ved Mjøsas bredd på Skreia i Innlandet er renholdsselskapet Sullestad Support AS lokalisert.

Selskapet har 24 ansatte. Hovedbasen er et tidligere festlokale som er omgitt av potetåkre og dyrkingsareal for løk, gulrøtter og korn.

En tidlig morgen i slutten av mai i fjor fikk daglig leder Gjermund Tolpinrund i Sullestad en melding fra en ukjent person som utga seg for å være en IT- mann med spesialkompetanse på hacking.

– Han spurte meg om vi hadde trøbbel med datasystemet vårt. Han påsto at han hadde funnet noen dokumenter om oss på det mørke nettet. Det var helt ukjent for meg, sier Tolpinrud.

Han sjekket først hvem som hadde ringt ham.

Det viste seg å være cybertrussel-ekspert Chris Culina i sikkerhetsselskapet Secunor. Han hadde mottatt tips om at dokumenter fra tre norske selskaper var å finne på det mørke nettet.

Tolpinrud logget seg på for å se om alt var greit.

– Jeg møtte en blå skjerm, og en beskjed om at alle våre data hadde blitt kryptert. Selv om jeg var forberedt,

fikk jeg helt noia. Det føltes som et personlig overgrep, jeg ble fullstendig paralysert, sier Tolpinrud.

– Det eneste vi sto igjen med var det vi visste vi skulle gjøre inneværende uke. Alle andre planer, kundeforhold og bestillinger var borte. Vi mistet alt. Det gikk helt på psyken løs.

– UFORSTÅELIG

Det viste seg at all data bedriften hadde var kryptert.

Sullestad fikk bistand av sikkerhetsfirmaet Secunor for å gjenoppbygge datainfrastrukturen, og tilgang til relativt ferske sikkerhetskopier ble redningen.

Ifølge sikkerhetsselskapet HackNotice, som monitorerer det mørke nettet, var det den russiske hackergruppa Prometheus som sto bak angrepet mot renholderselskapet.

– Jeg antar at de la igjen et løsepengekrav, men vi gikk ikke inn på noe som helst. At de angriper oss er uforståelig, og det viser at dette kan skje hvem som helst, sier Tolpinrud.

De ulike hackergruppene endrer jevnlig navn og strukturer – selv om medlemmene i flere av dem trolig er de samme. Det har ikke vært mulig å nå Prometheus for en kommentar til denne saken. Sullestad hadde innført to-faktorautentifisering og mener de bevisst hadde prioritert høy datasikkerhet.

– Vår IT-leverandør mente at vi var 100 prosent sikret. Likevel ble vi utsatt for dette. Det bør være en vekker for mange andre der ute, sier den daglige lederen i det lille renholdsfirmaet på Skreia.

LETER ETTER SIKKERHETSHULL

To dager seinere slo den samme russisk-linkede hackergruppen til mot et annet Toten-selskap, våpen- og ammunisjonsprodusenten Våpensmia. Selskapet leverer våpen og materiell til både Forsvaret og politiet.

Hva hackerne klarte å hente ut av selskapet er ukjent for Dagbladet og Kommunal Rapport. Daglig leder Ole Furuseth ønsker ikke å kommentere denne saken.

REPORTASJE

THOMAS FRIGÅRD
thomas@kommunal-rapport.no

TORGEIR P. KROKFJORD
tpk@db.no

NINA HANSEN
nina.hansen@db.no

– Dette er et tilbakelagt stadium for oss, sier han.

Cybertrussel-spesialist Chris Culina bisto både Sullestad og Våpesmia etter angrepene de ble utsatt for. Begge selskapene hadde den samme svakheten i sin datasikkerhet: En alvorlig sikkerhetsbrist i brannmuren som førte til at de ble offer for russiske hackere.

– For å opprettholde den datasikkerheten du ønsker deg, er det viktig å hele tiden å holde programvaren oppdatert. Kommer trusselaktørene først på innsida, er det som regel bare et spørsmål om tid før de oppnår det de kom for. Noen ganger skjer det i løpet av minutter, sier Culina.

Han mener at disse angrepene viser at det er uvesentlig om du befinner deg i en forstad i Ohio, en storby i Brasil, eller i et tidligere festlokale mellom poteter og løk på Toten.

– Toten er ikke et sted på Internett, og hackere våkner ikke opp og tenker «i dag skal jeg prøve meg på Toten.». De skanner hele Internett etter bestemte sårbarheter de kan utnytte, eller kjøper en ferdig liste med mål. Det er bare business, og det handler om å ikke være et enkelt mål, sier Culina.

LEDET KOMMUNEN PÅ SNAPCHAT

Knappe 10 kilometer lenger nord ligger tettstedet Lena, og her ligger rådhuset til Østre Toten kommune.

En lørdag morgen, en kald vinterdag i januar i fjor, registrerer kommunedirektør Ole Magnus Stensrud at det på kommunens Facebook-side varsles om trøbbel med datasystemet på sykehjemmet.

– Jeg tenkte at det kanskje bare var et strømbrudd, sier Stensrud til Dagbladet og Kommunal Rapport.

Snart kom det meldinger fra flere hold i kommunen om de samme problemene. Da gikk alarmen.

Det viste seg at samtlige av kommunens 1 300 ansatte hadde mistet tilgang til kommunens datasystem. Over 200 fagsystemer var satt ut av spill.

Kommunen hadde mistet kontroll over låsefunksjoner på sykehjemmene og alle andre kommunale bygg, de mistet oversikt over hva som befant seg i medisinskapene. De hadde ikke tilgang på pasientjournaler, søknader om sosialhjelp eller barnevernsdokumenter.

Bak det hele sto den russiske hackergruppa Pysa, går det fram av konsulentselskapet KPMGs gransking av angrepet.

Det har heller ikke vært mulig å nå denne gruppa for en kommentar. Angrepet mot Østre Toten var et av mange gruppa skal ha stått bak i 2021. I fjor høst anslo sikkerhetsbloggen Security Affairs at Pysa i november måned var den mest aktive av de russiske hackergruppene.

OVERVELDENDE

På Lena satte kommunedirektøren krisestab.

– Jeg forsto raskt at dette var alvorlig. Det

SLITASJE: Kommunedirektør Ole Magnus Stensrud sier hackerangrepet tæret kraftig på de ansatte.

PENN OG PAPIR: Da datasystemet ble tatt ned måtte kommunen styres ved hjelp av penn og papir. Det er det blitt mange permer av.

UNDER ANGREP: Slik kan de se ut når hackere har tatt over din PC. Foto: Privat

SPORENE TIL RUSSLAND

KASTET ALT: Da Raymond Elde skrudde på datamaskinen sin en arbeidsdag, fikk han store øyne. Foto: Privat

«Det er ingen som kan forstå konsekvensene av hacking før man selv har blitt vært et offer for det.»

RAYMOND ELDE, kringkastingssjef i Radio Nordkapp

var helt overveldende, men man går inn i en slags modus der du bare jobber for å finne løsninger. Liv og helse var vår første prioritet, sier Stensrud.

Det er uklart hva som var hackernes vei inn i kommunens datasystemer, men resultatet var at kommunedriften måtte over på penn, papir, Snapchat og Facebook.

– Det var spesielt å måtte ty til sosiale medier for å lede kommunen i en krisesituasjon, men vi måtte være kreative. Det fungerte faktisk ganske godt, sier Stensrud.

I et halvt år ble kommunen drevet på penn og papir.

– Det var mildt sagt utfordrende og krevende, men jeg må berømme de ansatte. De responderte fantastisk på situasjonen. Det ble funnet kreative og gode løsninger, og jeg tror ikke at dataangrepet gikk på bekostning av tjenestene vi leverte til innbyggerne, sier kommunedirektøren.

Hackerne lekket sensitive opplysninger om 156 personer på det mørke nettet. Kommunen har informert alle berørte om dette.

BETYDELIG SLITASJE PÅ ANSATTE

Kommunen har gjennom diverse back up-systemer klart å få tilbake all data og gjenoppbygge 98 prosent av de digitale løsningene som ble hacket. Over 1000 datamaskiner, over 200 fagsystemer, og 420 koblinger mellom systemene skulle gjenoppbygges.

Dataangrepet har kostet kommunen 35 millioner kroner i direkte kostnader. Da datasystemet var gjenoppbygget skulle over 170 kilo papirdokumenter skannes og registreres – før selve papirene ble makulert.

– Slitasjen på de ansatte har vært betydelig. De sto allerede i en krevende situasjon grunnet korona, sier Stensrud.

– Så kom dette.

Datatilsynet ga kommunen et gebyr på fire millioner kroner for brudd på personopplysningssikkerheten.

Kommunen erkjenner at datasikkerheten har vært for lavt prioritert, men en undersøkelse konsulentselskapet KPMG har gjort av datainnbruddet konkluderer med at sikkerheten trolig ikke var svakere enn for liknende kommuner i landet.

Nå er datasikkerheten til Østre Toten vesentlig styrket.

– DETTE UNNER JEG INGEN

Nesten 2000 kilometer nord for grønnsakjordene på Toten hadde kringkastingssjefen i Radio Nordkapp i fjor høst låst seg inn i radiolokalene i Honningsvåg. Kaffen sto klar, og det var bare å sette i gang morgensendingene.

Da han skrudde på datamaskinen, fikk han store øyne.

Noe var alvorlig galt.

Alle filer han hadde på maskinen hadde endret navn, og uansett hva han klikket på, så poppet den samme tekstboksen opp på hans skjerm med en lenke til en e-postadresse.

Radiokanalen var hacket. Det viste seg at hackerne hadde kryptert alle datafiler radiokanalen hadde i sitt system, inkludert back up-filene.

– Å innfri eventuelle pengekrav regner jeg med hadde medført nye krav, og man kan aldri være sikker på om datamaskinene blir rensket for virus. Vi valgte derfor å skrote alt vi hadde av datautstyr, og vi måtte starte helt på nytt, sier kringkastingssjef Raymond Elde.

Radiokanalen med tre ansatte og en omsetning på rundt to millioner ble offer for et løsepengeangrep med skadeprogramvaren Makop. Ifølge det anerkjente britiske cyberetterretnings-selskapet Orpheus, har Makop et russisk opphav. Dagbladet har forsøkt, også via sikkerhetseksperter, å finne ut hvem som står bak den skadelige programvaren – uten hell.

Etter angrepet har han fått et nytt syn på hvor viktig datasikkerhet også er for små aktører.

– Det er ingen som kan forstå konsekvensene av hacking før man selv har blitt vært et offer for det, sier Elde.

– Da ser man hvor avhengig man er av det man har lagret av data.

POTETER OG DATASIKKERHET

På Toten går livet sin vante gang.

Poteter, løk, gulrøtter og andre grønnsaker i ferd med å høstes inn, og kornsiloen i Lena er allerede fylt med 29 000 tonn korn.

I hundrevis av år har distriktet vært beryktet for sin unike evne til å dyrke førsteklasses grønnsaker.

Nå har Toten også satt datasikkerhet på kartet.

BLANK SIDE

HACKING

VI JAKTET HACKER-PENGENE:

– DRA TIL HELVETE

Dagbladet kan i dag avsløre hvordan den beryktede hackergruppa Killnet finansierer operasjonene sine. I en hovedrolle finner vi en motorsykkelbyggende, ultranasjonalistisk tidligere diamanthandler fra Moskva.

TORGEIR P. KROKFJORD
tpk@db.no
THOMAS FRIGÅRD
(Kommunal Rapport)

Ordlyden i meldingen vi mottar er illsint:

«Vi har videresendt spørsmålene dine til herr Logunov, og undersøkt hvordan sensasjonsblekka deres dekker det som skjer i Ukraina. Herr Logunov har bedt oss om å si følgende til deg: Dra til helvete!»

Meldingen, sendt på meldingstjenesten Telegram, er signert:

«Med all disrespekt / Hooliganz- og Killnet-gjengen.»

Raseriutbruddet etterlater flere spørsmål: Hvem er herr Logunov? Hva er Hooliganz?

Og hvilken forbindelse har det hele til hackergruppa Killnet, som hånet utenriksministeren og angrep norske myndigheter i juni?

Tjener penger

La oss først ta et steg tilbake og tenke oss en nyoppstartet virksomhet som trenger penger. Virksomheten kommer opp med flere måter å skaffe inntekter på:

- Sponsede innlegg på sosiale medier.
- Salg av effekter med firmalogoen.
- Donasjoner fra støttespillere, via 13 forskjellige betalingskanaler.
- PR-samarbeid med en kjent rapartist.

Kanskje høres det ut som en humanitær organisasjon? En kulturinstitusjon? Et gründerfirma?

Dagbladet kan i dag avsløre at dette er finansieringskildene til den beryktede, russiske hackergruppa Killnet.

Gruppa angrep norske myndigheter 29. juni, og er Vladimir Putins forlengede, kriminelle arm i invasjonskrigen i Ukraina.

Smykkemannen

Her kommer vi til «herr Logunov». Han heter Viktor, og har i sju år solgt smykker gjennom Hooliganz Jewelry i Moskva.

Stilen er lett gjenkjennelig for alle som har vært på rockefestival i Tyskland, et motorsykkeltreff eller et helgemarked på Youngstorget før gentrifiseringen tok av: Hodeskaller, våpen, svart og sølv.

Tidligere drev Logunov med diamanter. Nå driver han, i tillegg til Hooliganz Jewelry, ytterligere en nettbutikk. Der selger han klær og sko – og angrepskniver og økser. I sosiale medier pusher han erkenasjonalistiske innlegg og konspirasjonsteorier om invasjonen av Ukraina.

I juni dukket det opp flere nye smykker i Logunovs sortiment, som skilte seg ut blant biker-estetikken. Det var smykker med en stor K på, og smykker med ordlyden skrevet rett ut: KILLNET. På Hooliganz' side på VK – «russisk Facebook» – er forbindelsene til hackergruppa tydelige.

Flere innlegg hos smykkeprodusenten er undertegnet:

– VI ER KILLNET.

Så lenge russerne gjorde framskritt på slagmarken, kostet det over 4000 kroner å få en stor «K» på ringfingeren. 12. september, da ukrainske styrker slo tilbake i en voldsom motoffensiv, satte Hooliganz ned prisene med 20 prosent.

Det har de siste ukene kommet flere indikasjoner på at Killnet-kassa – kanskje – begynner å gå tom. Stadig hyppigere, og med stadig større bokstavstørrelse i meldingene, ber gruppa om donasjoner i kryptovaluta.

Samtidig gjennomfører gruppa fortsatt angrep i Putins tjeneste.

«Trollmannen»

Meldingstjenesten Telegram er Killnets viktigste kommunikasjonsplattform.

Over 100 000 personer følger gruppas ulike kanaler. Dermed kan det også være penger å hente på sponsede innlegg.

I praksis er sponsede innlegg at du betaler for at dine poster i sosiale medier skal bli sett av flere. Dagbladet bruker samme annonseform selv, det samme gjør tusenvis av andre norske virksomheter.

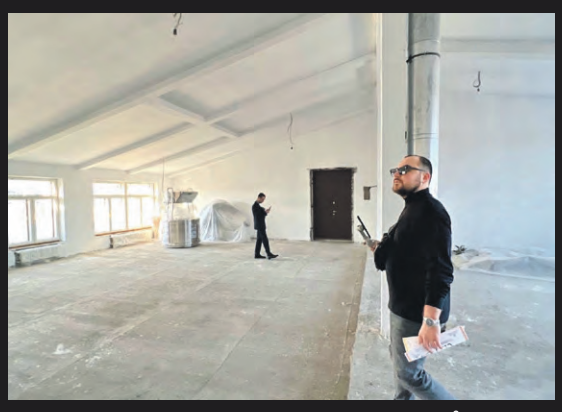
En som har annonsert hos Killnet er den innflytelsesrike eiendomsutvikleren og bloggeren Sergey Galler fra St. Petersburg.

Med over 140 000 følgere totalt på Telegram, VK og Instagram, livnærer Galler seg både som blogger, kursholder og eiendomsmegler. Totalt, hevder Galler, har han omsatt over 1000 leiligheter i St. Petersburg, Moskva og Dubai. Det er nok til at han selv, om seg selv, i et innlegg på VK stiller spørsmålet:

– Hvordan vet du at megleren din er en trollmann?

Om hans forbindelser til Killnet ikke rettferdiggjør «trollmann»-status også der, viser Dagbladets undersøkelser at eiendomsmagnet Sergej Galler er en bidragsyter til at Killnet kan bedrive sin kriminelle virksom- ➔

HACKING



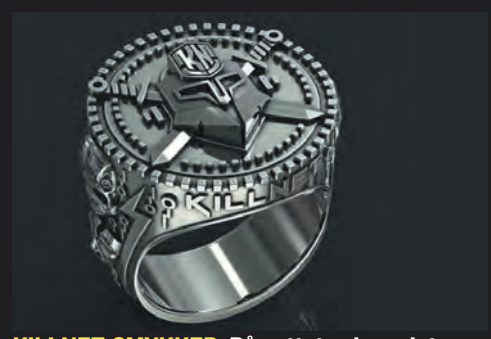
EIENDOMSMAGNAT: Sergey Galler hevder å ha solgt over tusen leiligheter. Foto: Privat

SMYKKEMANNEN: Viktor Logunov står bak smykkeprodusenten Hooliganz jewelry, som støtter hackergruppa Killnet. Han markedsfører også disse på sin egen profil. Foto: Privat

MANIPULERTE UTENRIKSMINISTEREN: Killnet angrep norske myndigheter i juni, de annonserte angrepet med et manipulert bilde av utenriksminister Anniken Huitfeldt.

RAPPER: Nå er Kaje Oboyma kalt inn på teppet hos utgiveren sin. Foto: Privat

GRÜNDER: Bakai Kolchaev reagerer på at en av hans artister støtter Killnet. Foto: Privat



KILLNET-SMYKKER: På nettet selges det smykker med en stor K på, og smykker med ordlyden skrevet rett ut: KILLNET. På Hooliganz' side på VK – «russisk Facebook» – er forbindelsene til hackergruppa tydelige.

«Vi har videresendt spørsmålene dine til herr Logunov, og undersøkt hvordan sensasjonsblekka deres dekker det som skjer i Ukraina. Herr Logunov har bedt oss om å si følgende til deg: Dra til helvete!»

→ het mot påståtte fiender av den russiske staten.

Hva Sergey Galler tenker om det, har han ikke ønsket å svare på. Galler har sett meldingene Dagbladet har sendt ham med spørsmål. Men ikke svart.

Rapperen

En annen ung, fremadstormende gründer er kirgisiske Bakai Kolchaev. Han er grunnlegger av plateselskapet Infinity Music, som har vokst til å bli en av de mest innflytelsesrike labelene for rap og hiphop i Russland og Kirgisistan.

Til sammen har selskapets Youtube-videoer flere millioner avspillinger. Blant Kolchaevs artister er den russiske rapveteranen Kaje Oboyma, også han fra St. Petersburg.

I juli slapp Oboyma låta «Killnet Flow» – en utilslørt hyllest til hackergruppa, komplett med vaiende russiske flagg i bakgrunnen. Musikkvideoen til låta innleder med amerikanske nyhetsankre som melder om russiske hackerangrep. Så følger latterliggjøring av Killnets «fiender» i den provestlige hackergruppa Anonymous, og skjermbilder fra Killnet-angrep mot italienske myndigheter.

Den engelskspråklige delen av teksten er kanskje litt banal, men låta setter seg unektelig på hjernen:

«Killnet, Killnet /Oh my gosh, oh shit.»

Hyllestlåta til de russiske hackerne ble gjort tilgjengelig på en rekke plattformer – blant dem både Spotify, Youtube og Apple Music.

Bakai Kolchaev skriver i en melding til Dagbladet at han skal undersøke saken – og at han ikke er komfortabel med situasjonen slik den er nå.

– Vi har jobbet med Kaje Oboyma I en årrekke og vært hans distributør, på samme måte som vi har vært det for kolleger av ham i St. Petersburg. Kaje har alltid vært kjent for hardtslående innhold, så sånn sett er ikke dette en overraskelse. Vi undersøker saken nå – publiseringen fungerer sånn at hvis innholdet ikke er i strid med reglementet på de digitale publiseringsplattformene, så går det automatisk ut. Vi skal ta opp saken på et møte hos oss nå, dette er en spesiell situasjon som vi ikke setter pris på, skriver Kolchaev.

Oboyma selv har ikke svart på Dagbladets spørsmål.

Hadde insider

Hvor mye omsetter Killnet for til sammen?

Dagbladet har over tid hatt kontakt med flere nåværende og tidligere medlemmer av Killnet – men det spørsmålet har de ikke ønsket å svare på. En av dem, «Oleg», opplyser imidlertid at han har en vanlig fulltidsjobb ved siden av aktiviteten i Killnet – og at hans motivasjon er utelukkende politisk.

Det tidligere Killnet-medlemmet «Igor» vil heller ikke komme med konkrete tall, men sier at både smykkesalg og sponsede innlegg gir gode penger:

– Jeg skal ikke si at det har vært veldig mange kjøpere av smykkene, men overskuddet var ikke dårlig. Det ble en bra inntektskilde for gruppa, sier «Igor».

– Hvordan kom dere i kontakt med Hooliganz?

– Når det gjelder smykkefirmaet hadde vi en person som jobbet der, som laget smykker for oss.

Solgte program for dataangrep

Gruppa kan også ha lagt seg opp litt penger fra oppstarten. Slik Dagbladet har fortalt, startet Killnet som en virksomhet som solgte programvare for DDOS-angrep – samme typen dataangrep gruppa selv er blitt beryktet for.

Ifølge bloggen til sikkerhetsselskapet SOC Radar annonserte Killnet programvare for en månedsleie på 1350 dollar – omkring 13 000,- kroner.

– Hva med sponsede innlegg i Telegram-kanalene deres, spør vi «Igor».

– Innimellom har vi slike annonser. Pengene går ikke bare til oss selv, men også til serverleie og andre ting, sier «Igor».

Dagbladet har søkt Killnet via deres konto på VK – russisk Facebook. Henvendelsen er ikke besvart. Henvendelser direkte til Viktor Logunov er ikke besvart. Hooliganz har ikke ønsket å utdype. Sergey Galler har ikke svart på Dagbladets spørsmål.

BLANK SIDE

HACKER-ANGREPET

Den russiske hackergruppa Killnet angrep Norge i juni. Nå kan Dagbladet avsløre at gru

Oppdaget skjult

TORGEIR P. KROKFJORD
tpk@db.no
NINA HANSEN (foto)
nha@db.no
CHRISTINA HOLEN KORNELIUSSEN (tv)
christina.korneliussen@db.no
THOMAS FRIGÅRD
(Kommunal Rapport)

Det var 29. juni at den russiske hackergruppa Killnet angrep Norge, gjennom såkalte Ddos-angrep mot en rekke offentlige myndigheter.

Opprinnelig var hackergruppa en produsent av skadelig programvare, men etter invasjonen av Ukraina har Killnet endret seg til å bli en selverklært del av Vladimir Putins russiske cyberarmé.

Angrepet på Norge er ett av flere angrep på Nato-land og «fiender av Russland».

Bitcoin-sporene avslører

Killnets angrep er teknisk sett ganske enkle, og velegnet til å skape frykt og støy – men gruppa er som regel ikke ute etter å presse ofrene for penger. Dagbladet har avslørt at gruppa derfor tjener penger på annonsesalg på meldingstjenesten Telegram, på salg av smykker med logoen deres på og på donasjoner i kryptovaluta – som bitcoin.

Hva kan vi finne ut om Killnet sin krypto-økonomi?

- Dagbladet kan nå avsløre at Killnet har overført bitcoin til kontoer der det står over en milliard kroner i kryptovaluta.
- Dagbladets undersøkelser viser at penger som Killnet bruker i den russiske cyberkrigen, har blitt overført til samme konto som penger fra organisert nettkriminalitet. Deriblant svindel som misbruker navnet til verdens rikeste mann.
- Dagbladet har både nå og tidligere søkt Killnet på deres eneste kjente sosiale medier-konto. Dagbladet har også sendt spørsmål til en russer vi har sporet opp som medlem av gruppa. Russeren har lest meldingen, men ingen av henvendelsene er besvart.

Narkoforumet

Vi begynner en formiddag i starten av september. Da chattet Dagbladet med «Igor», et tidligere medlem av den russiske hackergruppa Killnet, som vi hadde fått kontakt med i researchen til denne og andre artikler om hackergruppa.

Vi spurte «Igor» hva Killnet tjente penger på. Han svarte:

– Den gangen vi rundlurte SBU. Alt går igjennom bitcoin for oss.

«HER HØRES DET NESTEN UT SOM DE INVOLVERTE VIL BLI SPORET. FOR Å BEVISE AT EN TRANSAKSJON HAR FUNNET STED.»
COLIN BOYD, professor ved NTNU

SBU er den ukrainske sikkerhetstjenesten, og hendelsen «Igor» refererer til fant sted i august. Da ledet Killnet et større dataangrep mot nettforumet RuTor.

RuTor er et møtested på det mørke nettet, primært for salg av narkotika. Forumet ble angivelig driftet av nettopp ukrainsk etterretning.

Hendelsen er beskrevet på bloggene til flere anerkjente sikkerhetsselskaper – Flashpoint og Trustwave blant dem.

Løsepenger

«Igor» hevdet Killnet fikk løsepenger utbetalt i bitcoin etter dataangrepet. Det ryktet har sirkulert i bransjemedier siden august, men har ikke blitt verifisert.

I utgangspunktet bruker mange bitcoin (BTC) nettopp fordi de ønsker å være anonyme. For skal ikke kryptovaluta egentlig være umulige å spore?

I researchen til denne artikkelen kontaktet vi flere eksperter. Og det var professor Colin Boyd ved NTNU, som påpekte:

– Her høres det nesten ut som de involverte vil bli sporet. For å bevise at en transaksjon fant sted.

Tre adresser

Alle bitcoin-transaksjoner logges på nettstedet Blockchain.com.

Når du klikker på en transaksjon, havner du på en oversiktsside som viser alle transaksjonene mottakeradressen har vært involvert i.

I meldingene på Telegram der de ber om donasjoner, oppgir Killnet selv to adresser støttespillerne kan sende bitcoin til: Vi kaller dem K1 og K2. I tillegg til disse, sendte «Igor» en bitcoin-adresse til Dagbladet der han hevder løsepengene fra RuTor-hackingen ble betalt. «Igor» henviste til tre konkrete transaksjoner.

➜ FORTS. NESTE SIDE

ppa har overført bitcoin til **kontoer der det står over en milliard kroner i kryptovaluta.**

hacker-milliard

STORE PENGER: Den russiske hacker-gruppa Killnet som angrep Norge og andre «fiender av Russland» har overført penger til kryptovaluta-kontoer der det står verdier for over en milliard kroner.

HACKER-ANGREPET

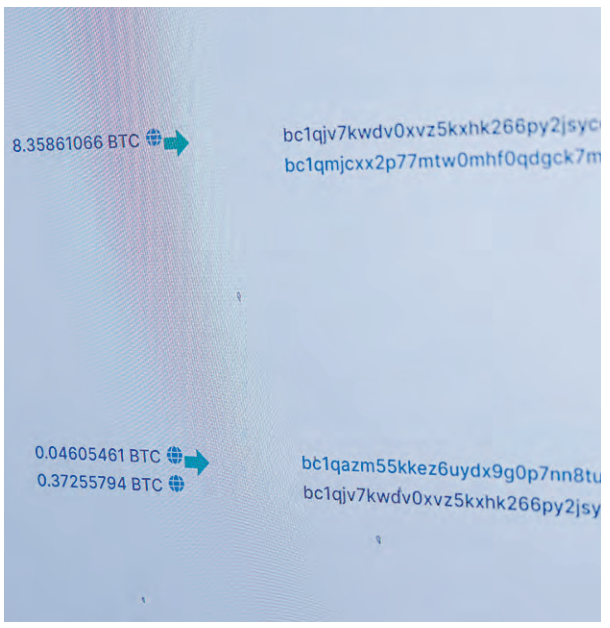
FAKTA

DETTE ER KRYPTOVALUTA

- Kryptovaluta er digital valuta som baserer seg på blokkjede-teknologi og desentralisert kontroll. Brukes i hovedsak til spekulasjon og investeringer.
- Det finnes rundt 2000 forskjellige kryptovalutaer – som Bitcoin, Ethereum, Ripple, Litecoin og Monero.
- Bitcoin var først ute, og ble lansert i 2009.
- Bitcoin kan sendes direkte mellom brukere digitalt.
- Oversikt over eiere av kryptovaluta, er lagret i en digital blokkjede, tilgjengelig for alle. Likevel er det ofte umulig eller vanskelig å identifisere eieren til kryptovaluta og hvem som var en del av en transaksjon. (NTB)

BITCOINSPORING: **Når du klikker på en bitcointransaksjon på nettstedet Blockchain.com havner du på en oversiktsside som viser alle transaksjonene mottakeradressen har vært involvert i.**

«ELON MUSK-SVINDEL»: **Penger fra såkalt «Elon Musk»-svindel skal ha gått inn på samme konto som Killnet-pengene.**



SLIK FANT VI PENGENE

Vi kaller de to kjente Killnet-adressene, adressene der gruppa selv har bedt om å få tilsendt penger, for K1 og K2.

På Blockchain.com går det fram at K1 og K2 totalt har mottatt henholdsvis 1,03 og 0,016 BTC. Med dagens kurs er det omkring 200 000 kroner. Det beløpet, som trolig stammer fra donasjoner, er ikke avskrekkende.

La oss gå videre. Hva kan vi finne ut om K3, adressen som «Igor», det tidligere Killnet-medlemmet, påsto tilhørte gruppa?

De undersøkelsene blir hakket mer kompliserte, men vil si oss mer om Killnets pengestrømmer.

De tre transaksjonene som ifølge «Igor» var bevis for at RuTor-forumet hadde overført penger til Killnet, var på (henholdsvis 0.09, 0.37 og 0.23 BTC – totalt 0,69 BTC) til sammen drøyt 141 000 kroner.

Ved å følge disse transaksjonene finner vi dokumentasjon for at «Igor» trolig snakker sant, når han hevder at Killnet fikk løsepenger fra RuTor-forumet. Via et mellomstopp havner nemlig den tredje delen av de påståtte løsepengene – 0,23 bitcoin – til slutt på Killnet-adresse K1. Dermed kan vi slå fast at Killnet mottok i hvert fall deler av pengene som «Igor» henviste til.

Så fulgte vi sporene fra K3 videre, til pengestrømmen til slutt stoppet opp. Det gjorde den, på kontoene der det står til sammen omkring en milliard kroner i bitcoin.

➜ FORTS. FRA FORRIGE SIDE

Dagbladets undersøkelser startet dermed med tre bitcoin-adresser som Killnet – angivelig – kunne knyttes til:

De to adressene der de selv ber om donasjoner. Og adressen som «Igor» hevder beviser at de fikk penger etter hackingen av RuTor.

Eksperten

Dagbladet har gått igjennom alle transaksjoner som går ut fra, og mellom, de tre kontoene.

Undersøkelsene styrker sannsynligheten for at «Igor» snakker sant, at Killnet faktisk fikk løsepenger fra nettforumet RuTor. Det har nemlig gått bitcoin fra en av kontoene som Killnet selv erkjenner å disponere – til kontoen «Igor» la fram for Dagbladet.

For å dobbeltsjekke at undersøkelsene vi gjorde hadde noe for seg, kontaktet vi kryptoanalyseselskapet Arcane Crypto.

Anders Helseth, senioranalytiker i selskapet, bekrefter at det er en forbindelse mellom de to adressene som Killnet ber om donasjoner til – og adressen som «Igor» nevnte overfor Dagbladet.

– De tre transaksjonene du henviser til, gikk alle til samme angivelige Killnet-adresse. Disse ble så sendt videre til andre adresser. Hvorav noe går til en av de to kjente Killnet-adressene via ett mellomhopp, sier Helseth.

Sammen med Dagbladet har Anders Helseth undersøkt Killnet-transaksjonene videre.

– Hackernes bitcoin danser i sirkler rundt halve internett, noe som også er poenget for å gjøre sporingen mer krevende. Det de gjør er å gruppere sine bitcoin sammen mange andres for deretter å gjøre en masse transaksjoner med de grupperte bitcoinene. Da er det veldig vanskelig å si hvem som er hvem sine til slutt. Men jeg fant to adresser disse Killnet-overføringene – på 0.69 BTC – sannsynligvis har endt opp i eller vært innom basert på transaksjonssporet og overføringsverdiene, sier Helseth til Dagbladet.

Milliardfunnet

– Den ene står det nesten 5000 bitcoin på nå – noe som tilsvarer 87 millioner dollar. Den andre står det snaut 60 bitcoin på nå.

– Forklar leserne: Hvordan kom vi fram til dette?

– Det vi nå har gjort er å følge pengene fra de adressene som vi vet, i hvert fall med ganske stor sikkerhet, tilhører Killnet.

Helseth fortsetter:

– Det er da løsepengeadressen, og de to donasjonsadressene deres. Så har vi fulgt disse pengene innom veldig mange adresser, som det heter i bitcoin, der pengene sendes ofte og til nye adresser. Dette sporet sprer seg som et tre med greiner. Når vi har fulgt en vei av dette sporet, så ender vi opp på adressene der det står bitcoin til en verdi av omkring 80 millioner dollar. En snau milliard kroner.

Elon Musk-svindel

Google-søk på de aktuelle bitcoin-adressene, indikerer at de har blitt brukt i en rekke former for nettsvindel.

På flere diskusjonsforumer er det medlemmer som skriver at en av adressene er brukt i såkalt «Elon Musk»-svindel.

Det er en form for bedrageri som jevnlig sirkulerer på sosiale medier. Ikke minst på Twitter,som Elon Musk nå selv eier.

Svindelen går ut på at annonser hevder at Musk eller Tesla har utviklet en ny kryptovaluta, som nå er til salgs. I enkelte annonser har såkalt «deepfake»-teknologi blitt brukt til å lage videoer, der en forsøksvis troverdig kopi av Musk. Med i overkant robotaktig stemme skryter den falske Elon Musk av den falske kryptovalutaen.

– Yikes. Definitivt ikke meg, skrev Musk selv på Twitter om en slik video.

Støtter Russlands invasjon

Hvis du likevel gikk på limpinnen, havnet pengene dine på en av de to bitcoin-adressene som også har tatt imot penger fra Killnet. Penger fra Elon Musk-svindel i sosiale medier ser dermed ut til å ende opp samme sted som en av inntektskildene til cyberkrigføringen til støtte for Russlands invasjon av Ukraina.

– Hva kan du bruke bitcoin til?

– Det du kan gjøre med dem, er at du kan bruke dem til å betale med. Men det er jo langt færre ting du kan kjøpe med bitcoin sammenliknet med vanlige penger. Det er eksempelvis veldig vanskelig, tilnærmet umulig, å gjøre bitcoin om til et hus, uten å gå via vanlige penger først. Men i internettverdenen, der mange av disse hackerne lever, er bitcoin generelt godtatt som betaling. Om du for eksempel har hackere tilknyttet deg, kan du betale dem lønn i bitcoin, sier Helseth.

«HACKERNES BITCOIN DANSER I SIRKLER RUNDT HALVE INTERNETT, NOE SOM OGSÅ ER POENGET FOR Å GJØRE SPORINGEN MER KREVENDE.»

ANDERS HELSETH, senioranalytiker i kryptoanalyseselskapet Arcane Crypto

BLANK SIDE

HACKER-ANGREPET

INGEN SPOR: Det var ingen spor å se etter Ifinex – eierselskapet til Bitfinex – oppgir på De britiske Jomfruøyer. Det opplyser Dagbladets lokale medarbeider. Foto: Zarrin Ahmed

Den russiske hackergruppa Killnet angrep Norge i juni. Nå kan Dagbladet avsløre at gruppa har overført bitcoin til kontoer der det står over en milliard kroner i kryptovaluta.

Oppdaget skjult hacker-milliard

«HER HØRES DET NESTEN UT SOM DE INVOLVERTE VIL BLI SPORET. FOR Å REVISE AT EN TRANSAKSJON HAR FUNNET STED.»

DAGBLADET: 24. november

Dagbladet kan avsløre at penger fra svindel- og hackerangrep i Norge, har gått via en kryptobørs i skatteparadiset De britiske Jomfruøyer. Bak står en kontroversiell italiener.

HIT GIKK DE SKJULTE PENGENE

ROAD TOWN/OSLO (Dagbladet):

September 2018: «Det vil bli publisert bilder av deg der du onanerer, hvis du ikke betaler bitcoin til oss.»

Slik lød en trussel som dukket opp i norske e-postbokser høsten 2018. Omfanget var såpass at Kripos så seg nødt til å advare mot virksomheten. Hvem som sto bak, eller hvor svindelpengene havnet, fant politiet aldri ut.

• Januar 2021: 15 måneder seinere sendte Finanstilsynet i Norge ut en advarsel mot en rekke selskaper. Blant dem var et selskap som, ifølge Finanstilsynet i Belgia, svindlet nettbrukere i hopetall.

• 29. juni 2022: 1,5 år etter det igjen, om morgenen 29. juni i år, var nettkriminalitet den største saken i det norske nyhetsbildet. Da meldte Dagbladet at den russiske hackergruppa Killnet angrep norske myndigheter, som svar på at Norge sa nei til transport fra Russland til Barentsburg på Svalbard.

Dagbladet kan i dag avsløre at de tre hendelsene har noe til felles: I samtlige saker skal det ha blitt overført kryptovaluta til en kontroversiell kryptobørs i Karibia.

Ukraina slo alarm

Kryptobørsen heter Bitfinex. Fra sin registrerte adresse i skatteparadiset De britiske Jomfruøyer, er den en av verdens viktigste vekslingssteder for kryptovaluta.

Bitfinex markedsfører seg direkte mot russere ved å la alle tjenestene være tilgjengelige på russisk. Ukrainske myndigheter ba allerede i mars om at Bitfinex skulle slutte å ta imot russiske penger.

Nå kan Dagbladet avsløre at en donasjon til Killnet har gått inn på kryptobørsen Bitfinex så seint som i september.

I en e-post til Dagbladet hevder Bitfinex først at det bare er en enkelt Killnet-relatert transaksjon som har vært innom deres systemer. På oppfølgingsspørsmål medgir imidlertid selskapets kommunikasjonssjef at det også flere enn denne ene transaksjonen, er på et tidspunkt er innom Bitfinex sin kryptobørs.

– Bitfinex har strenge retningslinjer for å motvir-

→

HACKER-ANGREPET

SJEFEN: Finansdirektør Giancarlo Devasini er ifølge Financial Times mannen som styrer kryptobørsen Bitfinex. Han har ikke selv svart på Dagbladets henvendelser om at hackerpenger skal ha blitt overført til hans kryptobørs. Foto: Bitfinex

KRYPTOBØRS: Innloggingen til Bitfinex fotografert på en smarttelefon. Penger fra flere kriminelle handlinger i Norge er overført til børsen. Foto: Rafael Henrique / SOPA Images / Shutterstock

«NÅR ALT KOMMER TIL ALT, ER DET JEG SOM STYRER SJAPPA I BITFINEX.»

GIANCARLO DEVASINI

ke hvitvasking, terrorfinansiering, brudd på sanksjonslover eller annen kriminell aktivitet. Vi går lengre enn det vi strengt tatt trenger for å motvirke slik aktivitet – det gjelder også alle uønskede aktører relatert til krigen mellom Russland og Ukraina, skriver Sheel Kohli, kommunikasjonssjef i Bitfinex, i en e-post til Dagbladet.

Dagbladet har også kontaktet selskapets italienske finansdirektør – den tidligere plastikkirurgen Giancarlo Devasini, som ifølge Financial Times er Bitfinex' sterke mann. Han har ikke svart på Dagbladets spørsmål.

En lokal medarbeider, Zarrin Ahmed, har på oppdrag fra Dagbladet oppsøkt adressen til Ifinex, eierselskapet til Bitfinex, på De britiske Jomfruøyer. Ifølge henne var det ingen spor å finne etter selskapet.

Mistenkelig

Først: Hva er en kryptobørs?

– Om du har bitcoin og vil ha dem ut i dollar, kroner, rubler eller hva som helst, er den vanligste måten å gjøre det på å sette dem inn på en børs og så selge dem, sier Anders Helseth til Dagbladet.

Han er senioranalytiker i kryptoanalyseselskapet Arcane Crypto, og har bistått Dagbladet i undersøkelsene av Killnets bitcoin-økonomi.

– På en kryptobørs kan du få det folk tenker på som vanlige penger. Det hackerne ikke kan gjøre er å selge veldig mye kryptovaluta på en gang, da vil de avsløre hvem de er. Børsene vil da rapportere at det er noe mistenkelig som foregår, sier Helseth.

Sporene til Bitfinex dukket opp i en større kartlegging av hackergruppa Killnet sin bitcoin-økonomi. Dagbladet avslørte at Killnet har overført bitcoin til kontoer der det står bitcoin verdt over en milliard kroner. Verken Killnet eller et av medlemmene deres ønsket å kommentere saken.

Dagbladet avslørte også at kontoene også ser ut til å ha blitt brukt i nettsvindel og annen kriminalitet tidligere – blant annet en form for investeringsbedrageri der Elon Musk, verdens rikeste mann, misbrukes for å svindle folk for penger.

– Det jeg tipper disse hackergruppene gjør, sier Anders Helseth.

– Er at de både bruker kryptovalutaen i en slags kryptoøkonomi – som er rundt disse hackergruppene. Og at de så gradvis veksler kryptovalutaen til ordinær valuta, på ulike børser, sikkert med falske identiteter – som de kanskje har hacket til seg. Da får de konvertert litt, så de får kjøpt seg mat og fine biler. Men mye blir værende i hacker-økonomien.

KRYPTOEKSPERT: Anders Helseth er seniorrådgiver i kryptoanalyseselskapet Arcane Crypto. Foto: Nina Hansen

FAKTA

KRYPTOVALUTA

- Kryptovaluta er digital valuta som baserer seg på blokkjede-teknologi og desentralisert kontroll.
- Brukes i hovedsak til spekulasjon og investeringer.
- Det finnes rundt 2.000 forskjellige kryptovalutaer – som Bitcoin, Ethereum, Ripple, Litecoin og Monero.
- Bitcoin, den mest kjente kryptovalutaen, var den første i sitt slag da den ble lansert i 2009.
- Bitcoin kan sendes direkte mellom brukere digitalt, uten å gå gjennom en bank eller andre mellommenn, og uten å be noen om lov.
- En oversikt over hvem som er eier av kryptovaluta, er lagret i en digital blokkjede som er tilgjengelig for alle.
- I mange tilfeller er det likevel umulig eller vanskelig å identifisere eieren til kryptovaluta og hvem som var en del av en transaksjon.

(NTB)

«Hot wallet»

Nå kan Dagbladet altså avsløre at en av de to kontoene der Killnets penger stoppet, tilhører Bitfinex.

At kontoen tilhører Bitfinex går fram av en omfattende artikkel om Bitfinex og deres egen kryptovaluta Tether, publisert i forskningstidsskriftet The Journal of Finance i oktober 2019. Kontoen er også navngitt i flere innlegg fra kryptoanalytikere på nettforumene Twitter og Reddit.

Kontoen er en såkalt «hot wallet» – noe som betyr at den er tilknyttet Internett hele tida. Det gjør det lettere å overføre penger inn og ut av kontoen, men det gjør den også mer sårbar for hacking. En «cold wallet» er derimot ikke koblet til nettet. Noe som gjør den sikrere, men også mer kronglete å bruke.

At det kan medføre risiko å ha kryptovaluta stående hos Bitfinex, gikk fram i 2016. Da ble kryptobørsen utsatt for et av tidenes mest innbringende hackerangrep. Samtidig skal et stort antall mistenkelige transaksjoner ha funnet sted. Et amerikansk ektepar ble i februar i år pågrepet i saken, siktet for forsøk på å hvitvaske bitcoin – stjålet fra Bitfinex – verdt 32 milliarder kroner.

Flere transaksjoner

Sheel Kohli, kommunikasjonssjef i Bitfinex, skriver i en e-post til Dagbladet:

– Vi har nøye undersøkt påstandene om at penger fra en av Killnets donasjonskontoer har blitt overført gjennom Bitfinex' «hot wallet», og vi har funnet at dette ikke er tilfelle. «Midlene» det er snakk om er en enkelt transaksjon, utført i september 2022, verdt totalt 166,27 dollar. Pengene stammer fra en donasjon til Killnet, som var innom to andre kontoer mellom donasjonsadressen og Bitfinex sin «hot wallet».

– Killnet opererer minst tre bitcoin-kontoer, med mye trafikk ut og inn. Kan du garantere at denne transaksjonen er den eneste?

– Vi er klar over, som du korrekt påpeker, at Killnet har minst tre donasjonskontoer. På alle er det et høyt antall inngående og utgående transaksjoner. På samme måte som den spesifikke transaksjonen vi kommenterte i vårt forrige svar, er noen av disse andre transaksjonene innom Bitfinex indirekte.

Sheel Kohli presiserer at dette skjer gjennom en rekke mellomstopp, som trolig i enkelte tilfeller administreres av andre kryptobørser, betalingstjenester eller kryptomeklere. Han hevder at ingen av transaksjonene « berører Bitfinex direkte».

– Det har ikke vært direkte kontakt mellom Killnet og vår kryptobørs. Killnet har ikke hatt mulighet til å vaske penger hos oss.

– Vi har en rekke tiltak vi kan sette inn, om vi mistenker at noen bruker vår plattform til kriminell aktivitet. Vi har også mulighet til å fryse midler eller frata noen kontoene deres.

Italiener står bak

Selv om han på papiret «bare» er finansdirektør, er det ifølge Financial Times italieneren Giancarlo

Devasini som er Bitfinex' sterke mann. Et lekket taleopptak fra 2016, som avisa refererer, indikerer det samme.

Der sier italieneren:

– Når alt kommer til alt, er det jeg som styrer sjappa i Bitfinex.

Italieneren er opprinnelig plastikkirurg, et yrke han ifølge Financial Times la vekk fordi han ganske raskt kom til en erkjennelse om at «alt jeg gjorde var å svindle folk».

Devasini har vært innom flere bransjer – og en rekke ganger vært i klammeri med politi og påtalemyndigheter. Men innen kryptovaluta har Devasini det siste tiåret blitt en av de virkelig store.

Kryptoprofilen Sam Bankman-Fried, som nå selv etterforskes, etter at kryptobørsen hans FTX kollapset, har overfor Financial Times karakterisert Devasini slik:

– Han er på 24/7. Han håndterer ikke bare kriser eller store muligheter, men den daglige operasjonen. Devasini legger masse stolthet i det han har bygget opp i Bitfinex og Tether (en kryptovaluta tilknyttet Bitfinex). Samtidig blir han irritert av folk han mener slenger dritt om virksomheten hans uten grunn.

Devasini har lest WhatsApp-meldinger med spørsmål fra Dagbladet, men har ikke svart på spørsmålene.

Klagene

Hva er koblingen mellom Bitfinex og den norske nettsvindelen?

Indikasjoner på det finner vi på nettstedet Bitcoin Abuse. Som med nettsteder, er det mulig å klage inn bitcoin-adresser du mener brukes av kriminelle. Nettsteder kan rapporteres til for eksempel Slettmeg.no, mens bitcoin-adresser kan rapporteres til for eksempel Bitcoin Abuse.

Ingen hos Bitcoin Abuse har ønsket å kommentere denne saken.

Men i oversikten deres over brukerklager, finner vi at begge Killnet-adressene er klaget inn en rekke ganger. Klagerne oppgir at de to adressene skal ha blitt brukt i grov nettsvindel.

Alle rapportene er anonyme. Men ofrene hevder seg utsatt for følgende:

– Flere former for utpressing

– Investeringsbedrageri, som lurer ofrene med på pyramidespill og liknende

– Hacking med såkalt trojanervirus, som infiserer ofrenes datamaskin

– Såkalt «sextortion», altså utpressing som lurer ofrene til å tro at intime bilder av dem er på avveie.

Flere av klagerne oppgir at de er norske. De påståtte norske ofrene advarer også mot såkalt investeringsbedrageri, der de, lures til å investere i næringsvirksomhet, valutaspekulasjon og pyramidespill som ikke er annet enn lureri. Andre ofre oppgir å bo i USA, Nederland, Indonesia, India og Portugal.

Bitfinex har ikke svart på spørsmål om nettsvindel-selskapene.

Raser: – Kriminelle jævler

Fra Indonesia rapporterer en av klagerne:

– Jeg har fulgt «du har blitt hacket»-e-postsvindelen. Det har kommet penger til denne kontoen [« hot wallet»-kontoen hos Bitfinex] fra omkring ti andre adresser.

Et offer som oppgir å være fra Norge, er rasende:

– Vær obs på disse kriminelle jævlene. De svindler folk med falske selskaper.

I klagen, som ble sendt inn i september 2019, navngir brukeren to selskaper. Hvorav ett – med navnet OTPFX – påstås å være knyttet til tidligere svindeltransaksjoner. Finanstilsynet i Norge gikk et drøyt år seinere ut og advarte mot det samme selskapet. Selskapets nettsider er nå nede, og det framstår ikke som aktivt lenger.

– Markedsadvarselen på Finanstilsynets nettside er en publisering av en advarsel fra den belgiske tilsynsmyndigheten. Selskapet har heller ikke tillatelse til å yte konsesjonspliktige tjenester i Norge, skriver tilsynsrådgiver Jo Singstad i Finanstilsynet i en e-post.

Dagbladet har forsøkt å få kontakt med OTPFX, uten hell. Kripos bekrefter overfor Dagbladet at de ikke vet hvem som sto bak e-postsvindelen.

KRYPTOEKSPERT: Sebastian Claydon Takle.

– KRYPTO ER VIKTIG FOR KRIMINELLE

I Bjørvika sitter Sebastian Claydon Takle, leder for Financial Cyber Crime-senteret til DNB – som i 2021 håndterte rett i underkant av 8400 bedrageritilfeller, verdt rett under en milliard kroner.

Når han blir forelagt Dagbladets funn, bekrefter Takle at kryptovaluta er et viktig redskap for nettkriminelle.

– Kryptovaluta har blitt sentralt for mange av miljøene bak bedragerier. Igjen, så velger disse aktørene enkleste vei til mål og krypto forenkler noen av prosessene. Det ene er å skjule midlenes opprinnelse. Det å flytte penger ut av den vanlige finansielle infrastrukturen er en av mange måter å vanskeliggjøre sporing av midler, sier Takle til Dagbladet.

BLANK SIDE

HACKER-ANGREPET

UKRAINA VIL TA AFFÆRE

Dagbladet tirsdag 6. desember

Ukrainske myndigheter reagerer kraftig på Dagbladets avsløringer om bitcoin-økonomien til den beryktede russiske hackergruppa Killnet. Norske eksperter slår alarm.

TORGEIR KROKFJORD
tpk@db.no

REAGERER: Statssekretær Oleksandr Bornyakov i det ukrainske digitaliseringsdepartementet reagerer sterkt på Dagbladets avsløringer om bitcoin-økonomien til den russiske hackergruppa Killnet. Foto: Ministry of digital transformation of Ukraine

Vi vil helt klart reagere på disse mulige bruddene på internasjonale sanksjoner. Det sier statssekretær Oleksandr Bornyakov i det ukrainske digitaliseringsdepartementet til Dagbladet. Han er stedfortrederen til Ukrainas digitaliseringsminister Mykhajlo Fedorov – som igjen er visestatsminister i landet.

Bornyakov reagerer sterkt på Dagbladets avsløring av at bitcoin fra den russiske hackergruppa Killnet – som har angrepet blant annet norske myndigheter – har gått via den store kryptobørsen Bitfinex på De britiske Jomfruøyer.

– Russland begår et reelt folkemord i Ukraina. Det er ikke lenger rom for at virksomheter kan være «nøytrale». Selv om teknologien selv er nøytral, bør ikke folkene som står bak teknologiselskapene være det, sier Bornyakov.

– Sterke indikasjoner

Han sier at det er vanskelig å hindre at russiske hackere tar i bruk åpne, tekniske løsninger. Men sier det er viktig å gjøre det så vanskelig som mulig for grupper som Killnet og andre selvtitulerte medlemmer av Russlands cyberhær. Han navngir ingen selskaper. Videre slår han fast:

– Om et selskap har som mål å drive virksomheten sin på en etisk måte, må selskapet selv prioritere fred og etikk – og ikke støtte den russiske krigsmaskinen, uansett på hvilken måte dette skjer.

Bitfinex er forelagt Ukrainas uttalelser, men har ikke ønsket å gi ytterligere kommentarer. Selskapets kommunikasjonssjef Sheel Kohli har overfor Dagbladet vært tydelig på at selskapet mener Killnet ikke har hatt mulighet til å vaske penger gjennom deres kryptobørs.

Norske eksperter mener Dagbladets funn om Killnet sin bitcoin-økonomi, kan vise et nytt russisk mønster. De advarer norsk politi. Dagbladet avslørte at svindelaktører som har vært aktive i Norge har overført penger til den samme kontoen hos Bitfinex som det Killnet gjorde.

Kan vaskes til penger

Dagbladet vet ikke om det russiske hackermiljøet og personene bak svindlene har noe med hverandre å gjøre. Men det de har til felles, er at bitcoin de overfører gjennom Bitfinex, kan vaskes til vanlige penger og gå inn i den hvite økonomien.

– Dette kan tyde på at Russland har gått fra først og fremst fokusere på cyberangrep for sabotasje og påvirkningskampanjer til også å fokusere på økonomisk vinning gjennom cyberaktiviteter, sier Niels Nagelhus Schia, seniorforsker ved NUPI og leder for Forskningsgruppen for sikkerhet og forsvar.

> **«DETTE KAN TYDE PÅ AT RUSSLAND HAR GÅTT FRA FØRST OG FREMST Å FOKUSERE PÅ CYBERANGREP FOR SABOTASJE OG PÅVIRKNINGSKAMPANJER TIL OGSÅ Å FOKUSERE PÅ ØKONOMISK VINNING GJENNOM CYBERAKTIVITETER.»**
> **NIELS NAGELHUS SCHIA,** seniorforsker ved NUPI

– Viktigheten av pressens rolle i å tydeliggjøre kriminalitetens omfang og metoder står for meg som mye tydeligere etter å ha lest dette, sier Espen Johansen, sikkerhetsdirektør i IT-konsernet Visma, til Dagbladet.

Peker på politiet

– Artiklene bekrefter observasjoner Visma har gjort de siste åra. Spesielt siden de viser hvor store ressurser cyberkriminelle virker å ha til disposisjon.

Han vil problematisere om politiet har ressurser nok til å etterforske svært kompliserte cyberkriminalitetssaker.

– Visma anser politiet i Norge som svært kompetente og interesserte i denne formen for kriminalitet. Vi samarbeider godt med norsk og internasjonalt politi. Men vi er usikre på om politiet har kapasitet til å håndtere det volumet som våre etterretninger indikerer at står foran oss. Vi ser ikke dette som et særnorsk fenomen og vet at innhenting, analyse, etterforskning, og forfølgelse er svært teknisk komplisert, sier Espen Johansen.

FAKTA

HACKERANGREPENE

- Hacker-gruppa Killnet angrep norske myndigheter i juni.
- Dagbladet har i en rekke artikler avslørt hvordan Killnet tjener penger på en rekke ulike måter, også ved hjelp av lovlige virksomheter.
- Dagbladet har funnet bakmenn til denne finansieringen på Kypros.
- Dagbladet har også avslørt at kryptovaluta fra Killnet har gått gjennom den store kryptovaluta-børsen Bitfinex. Dette mener Ukraina kan være brudd på internasjonale sanksjoner.

SERVERTE STJERNENE –VAR FRYKTET HACKER

På nettet skjuler de beryktede, russiske hackerne seg bak masker og falske navn. Dagbladet kan i dag avsløre hvem som skal skjule seg bak maskene.

TORGEIR P. KROKFJORD
tpk@dagbladet.no
OLEG GRABENKO
oleg.grabenko@db.no
THOMAS FRIGÅRD
Kommunal Rapport

Jeg skal fortelle deg en ting, min kjære medborger. Jeg finner deg hvor som helst.

Mannen går mot rulletrappa på flyplassen, og snakker mot mobilkameraet sitt. Så vender han mobilen ned, og snikfilmer rumpa til dama over ham i trappa. Mannen gir uttrykk for å like det han ser, før han fortsetter monologen, med trusler til en ukjent adressat.

– Du er ferdig. Forstått?

ANGREPENE

Dagbladet og Kommunal Rapport har kartlagt nesten 50 dataangrep mot norske bedrifter og myndigheter. Den store majoriteten er utført av grupper med opphav i Russland.

To av de mest beryktede, russiske hackergruppene heter Conti og Revil. På verdensbasis anslås de å ha tjent hundrevis av millioner i løsepenger. I Norge har de angrepet virksomheter som Choice Hotels, Vard, Mobile, Imenco, Nortura og Inocean.

Samtidig har «russiske hackere» blitt en slags samlebetegnelse på ondsinnede datanerder som sitter på gutterommet og ødelegger folks liv. Hvem er de – sånn egentlig?

Flere av hackergruppene har vært rammet av datalekkasjer – og på den måten fått smake sin egen medisin. Påståtte navn, e-postadresser, IP-adresser og annen informasjon er lekket på sider som Github, Twitter, Reddit og IntelX. Dagbladet har analysert informasjon fra flere slike lekkasjer, og faktasjekket denne.

Ved hjelp av bildesøk, selskapssøk og informasjon fra russiske registre og rettspapirer, har Dagbladet luket ut en del navn på folk som feilaktig er hengt ut som hackere.

Men også kunnet fastslå identiteten til flere av de antatte hackerne.

Mannen som snikfilmer den intetanende kvinnens bak, er nemlig ikke en hvilken som helst fyr med mobiltelefon.

MANNEN MED FIRE FINGRE

På nett kaller han seg for «Wazawaka».

Med bare fire fingre på venstrehånda og en tidvis høy profil i sosiale medier, har han fått en viss kultstatus i IT-sikkerhetsmiljøet.

«Wazawaka» har stått bak de reineste tirader på Twitter, både om seg selv og andre i hackermiljøet. Det er også han selv som har lastet opp videoene Dagbladet omtaler i dag.

Ifølge en stor datalekkasje på Twitter, verifisert av det anerkjente sikkerhetsselskapet Recorded Future, skal «Wazawaka»

SPISEGJEST: Ralph Fiennes (t.h.) er en av prominensene som skal ha tatt for seg av bordets gleder på den antatte hacker-restauranten i St. Petersburg. Her med Meryl Streep ved et annet restaurantbord. Arkivfoto: NTB

ha vært involvert da hackergruppa Conti slo til mot myndighetene på Costa Rica.

Conti lammet hele datasystemet for skatt og tollinnkreving. Angrepet kostet costaricanske myndigheter 30 millioner dollar – pr. dag.

«Wazawaka» har ikke svart på Dagbladets spørsmål. Men han har sett og lest en henvendelse fra oss om intervju – før han så slettet meldingstråden. Når vi har ringt, har han lagt på.

Men i august ga han et sjeldent innblikk i hvordan invasjonen av Ukraina framsto fra et hacker-perspektiv.

– DREIT PÅ MEG

– Løsepengevirus-bransjen vil dø. Alt endret seg med «spesialoperasjonen» i Ukraina. Etter det har ofrene sluttet å betale.

Det hevdet «Wazawaka» i et intervju med bloggen The Record – som produseres av sikkerhetsselskapet Recorded Future. I intervjuet omtaler «Wazawaka» invasjonen av Ukraina konsekvent som en «spesialoperasjon» – i tråd med den russiske propagandalinja.

– Nå skriver folk til meg at jeg «er en russisk okkupant. Vær fornøyd med 10 000 dollar, dere får ikke mer». Fortjenesten har ramlet sammen det siste halve året. Det er blitt vanskelig å jobbe sånn generelt.

«Wazawaka» kommenterer også at Russland og USA – før invasjonen av Ukraina – for første gang samarbeidet om å ta hackere.

– Jeg dreit på meg og var veldig redd. Jeg drakk veldig mye i den perioden. Jeg leste meg opp på grunnloven og forsto det slik at de ville la meg bli i Russland [siden Russland ikke har noen utleveringsavtale med USA]. Men det var skummelt. Da spesialoperasjonen i Ukraina begynte, var jeg glad som faen. (...)

KOM MED SPARK

I sommer annonserte «Wazawaka» på Twitter at «jeg er tilgjengelig for spørsmål – send melding». Vi sendte ham en melding, men fikk ikke svar.

I åpne Twitter-innlegg ga han imidlertid kommentarer: Han kommenterte enkelte «trender» innenfor løsepengevirus-miljøet, som hvilke programmer de skadelige kodene skulle programmeres i. Han indikerte også at han er selvlært som hacker:

– Jeg er ingen utvikler, tvitret «Wazawaka».

«Wazawaka» kom også med et lite spark til enkelte sikkerhetsnettsteder som i samme periode postet en video av en ung mann bak rattet på en Porsche – og påsto det var «Wazawaka» som kjørte. Problemet, som han selv peker på:

Sjåføren har fem fingre på venstrehånda.

«Wazawaka» tvitret:

– Hei folkens, hvorfor lot dere dere lure av Porsche-gåten? Jeg lot en venn kjøre den

➜ FORTS. NESTE SIDE

«VI ER RESTAURANTEN DER BALLERINAENE FRA MARIINSKIJ-TARTAR ELLER GJØRS MED RØDBETE HOS OSS, VIL DU GJØRE

LIVREDD: Det kortvarige samarbeidet mellom USA og Russland om å ta russiske hackere, skapte frykt i miljøet. Foto: AP / NTB

➜ FORTS. FRA FORRIGE SIDE

mens jeg var borte – takk Gud for at han har alle fingrene sine fortsatt.

Det er de færreste av de antatte hackerne som har holdt en like høy profil som «Wazawaka». La oss gå på restaurant i St. Petersburg.

KUNSTNERNES MØTESTED

På et travelt gatehjørne, like ved det sagnomsuste Mariinsky-teateret i sentrum av St. Petersburg, ligger det en liten restaurant.

«Stengt permanent», får du beskjed om hvis du søker den opp på nettet nå. Det virker å være synd: Anmeldelsene på nett har et snitt på 4,6 av 5 mulige poeng. Gjestene skrøt av både god mat med en touch av Middelhavet og en mangfoldig vinliste.

På sin nå nedstengte nettside, skrøt restauranten av et rikt utvalg viner fra både Burgund, Rioja og Toscana. Eget lekerom for barna. Og hevder å ha kjendiser fra teatermiljøet på gjestelista:

«Vi er restauranten der ballerinaene fra Mariinskij-teatrene går. Hvis du bare en gang spiser biff tartar eller gjørs med rødbete hos oss, vil du gjøre som ballettdanserne og komme hit gang på gang. (...) Musiker Sergey Shnurov, komponist Rodion Shchedrin og skuespillerne Sergey Bezrukov og Ralph Fiennes er blant berømthetene som kom til oss for å spise middag.»

To kamerater sto bak den nå nedlagte restauranten, ifølge opplysninger fra det russiske selskapsregisteret. Ifølge russiske rettsdokumenter skal en av dem ha vært et medlem av hackergruppa Revil.

RESTAURATØREN

Revil har i Norge angrepet blant annet Vard – rederiet som lager E-tjenestens spionskip.

Tidligere skal han ha brukt en del tid på å spille krigsspill på nettet. Da han ble arrestert var restauratøren, ifølge russiske medier, en velstående ung mann. I tillegg til det fasjonable serveringsstedet, skal han også ha drevet et IT-selskap sammen med faren til medeieren i restauranten.

Dagbladet har gjentatte ganger forsøkt å få en kommentar fra den russiske advokaten Igor Vagin, som representerer en rekke antatte Revil-medlemmer – blant dem restauratøren i St. Petersburg. Advokaten har bekreftet at han har fått våre spørsmål, og har også sagt at han skal svare på dem. Men tross gjentatte purringer har svarene uteblitt. Dagbladet har også søkt restauratøren direkte – uten hell.

Han er bare ett eksempel på at de antatte medlemmene av Russlands mest beryktede hackergrupper, i mange tilfeller har jobber som ikke matcher ideen om Red Bull-drikkende einstøinger i joggebukse.

Men i januar hadde presidentene i USA og Russland snakket sammen. Ballettdanserne fra Mariinsky-teateret måtte finne et nytt sted å spise.

Etter flere store dataangrep mot amerikanske og internasjonale selskaper, krevde den amerikanske presidenten Joe Biden i fjor sommer at hans russiske kollega Vladimir Putin satte en stopper for angrep fra russiske hackergrupper.

FSB TIL AKSJON

I januar i år gikk så det russiske hemmelige politiet FSB til aksjon. 14 ble arrestert. Ifølge russiske medier er flere av de pågrepne studiekompiser fra St. Petersburg, som møttes da de bodde i samme hybelkompleks.

Flere av dem fikk forlenget varetekt til september. Det hindret ikke Revil i å bli operativ igjen, og gruppa har så seint som i november blitt knyttet til nye angrep.

Til avisa Kommersant har Igor Vagin tidligere foreslått at de antatte Revil-medlemmene skulle samarbeide med russiske myndigheter og bruke hacker-egenskapene sine, og informasjonen de hadde tilegnet seg, i statlig henseende.

GODE JOBBER

Myten om den ensomme datanerden styrkes ikke av Dagbladets gjennomgang av de mistenkte hackerne. Heller høres det følgende ut som deltakerlista i en litt spicy episode av NRKs «Hvem bor her? »:

– Den nevnte restauratøren fra St. Petersburg. En selvstendig næringsdrivende. – En mellomleder i offentlig sektor. En produktutvikler. Et tidligere idrettstalent med kulturelle interesser. En shippingutdannet levemann, med yrkeserfaring fra et bettingfirma og en forkjærlighet for vannpiper og champagne.

Med andre ord: flere av de antatte hackerne, har betrodde yrker i til dels store og velansette virksomheter. Det samme er tilfelle med medlemmer av hackergruppa Killnet, som Dagbladet intervjuet tidligere i år.

En av dem, som har en høy stilling i et stort firma i Russland, viste Dagbladet hvordan han hacket for Killnet fra mobilen mens han var på sin «hvite» jobb. Ingen av de nevnte antatte medlemmene av Revil og Conti har svart på Dagbladets henvendelser.

ETTERRETNINGSTJENESTEN

Et hyppig stilt spørsmål er hvorvidt det er noen forbindelse mellom hackergruppene og russisk etterretning og forsvar. Hva kan lekkasjene si oss om hvorvidt hackerne har militær bakgrunn?

I hacker-verdenen er utgangspunktet at målet er å bli rik – punktum. Politisk aktivitet har vært en sjeldenhet. Derfor vekket det oppsikt da Conti i februar sendte ut en melding på det mørke nettet, der de åpent erklærte sin støtte til Russlands invasjon av Ukraina.

I det lekkede materialet fra Conti går det imidlertid fram at det er motstridende syn på invasjonen internt i den kriminelle gruppa. Sikkerhetsselskapet Hold Security har publisert korrespondanse der hackeren Skippy skriver:

TEATRENE GÅR. HVIS DU BARE EN GANG SPISER BIFF SOM BALLETTDANSERNE OG KOMME HIT GANG PÅ GANG.»

FAKTA

HVOR KOMMER NAVNENE FRA?

- Navnene på de antatte hackerne stammer delvis fra russiske etterforskningsdokumenter – og delvis fra store lekkasjer av internt materiale fra de forskjellige hackergruppene.
- Slike lekkasjer sirkulerer på det mørke nettet fra tid til annen, og spres via ulike nettsider og nettjenester som Github, Reddit, Telegram og IntelX. '
- En del av materialet stammer fra en anonym Twitter-bruker, som i flere porsjoner har spredt påstander om identiteten til ulike hackere. Gjennom bildesøk og annen research har Dagbladet funnet at enkelte av de påståtte navnene virker å være feil.
- Eksempelvis var bildet av en person som ble påstått å være russisk hacker, hentet fra en nederlandsk datingside. Men av sikkerhetseksperter anses materialet i utgangspunktet å være pålitelig.
- – Jeg har hatt flere samtaler med vedkommende som står bak den aktuelle kontoen. Så vidt meg bekjent, har påstandene derfra vært velfunderte, skriver hacker-eksperten Soufiane Tahiri i en e-post til Dagbladet.
- Det samme opplyser journalisten AJ Vicens, som har dekket cybertrusler i en årrekke, i en e-post. Materialet som dukket opp i lekkasjene kan være at hackerne har brukt sine personlige e-postadresser, det kan være brukernavn på forum eller sosiale medier eller i noen tilfeller hackernes fulle navn. Dagbladet har også kontaktet personen bak Twitter-kontoen. Vedkommende ønsker ikke å gi noen kommentar.
- Dagbladet har også funnet store mengder lekket materiale om russiske hackere i søkemotoren IntelX, som gjør dypsøk blant annet på det mørke nettet.

SHIPPING: **På dette klassebildet fra et russisk shippingakademi, står en av de antatte hackerne blant elevene. Foto: Privat**

– Ting vil endre seg når det brenner bål på Den røde plass. (...) Kanskje Kreml til slutt går opp i flammer.

«Skippy» antas, ifølge en lekkasje på Twitter, å være i gruppas team som forhandler med ofrene for å få dem til å betale løsepenger. Contis problem var at flere av gruppas hackere var ukrainere. Som hevn, lekket en av disse store mengder intern informasjon.

MILITÆR ERFARING

På nett ble dokumentene kjent som «Conti Leaks». Slik Dagbladet har omtalt tidligere, inneholdt disse en rekke indikasjoner på kontakt mellom Conti og etterretningstjenesten GRU.

Dagbladet kan i dag avsløre at også flere av de antatte medlemmene av hackergruppene skal ha flere år bak seg i det russiske forsvarsapparatet.

«Begemot» er ett av kallenavnene en erfaren IT-frilanser fra St. Petersburg antas å bruke når han opererer sammen med Conti. Hans navn og e-postadresse dukker opp i en rekke lekkede Conti-meldinger, som Dagbladet har sett.

«Begemot» har ikke svart på en rekke henvendelser fra Dagbladet, men er tilsynelatende en fri mann – og på utkikk etter nye oppdrag. For bare noen uker siden redigerte han profilen sin på en stor rekrutteringsside, viser historikken på siden.

Profilen er krydret med rosende ord fra tidligere kolleger – det følgende er bare ett eksempel:

«Veldig teknisk dyktig. Løste et komplisert problem på bare noen få timer, som vårt team hadde brukt dager eller uker på.»

På en av nettprofilene oppgir «Begemot» selv at han har erfaring fra det russiske forsvaret. Det gjør også en antatt kollega av ham hos Conti – kjent under pseudonymet «elvira».

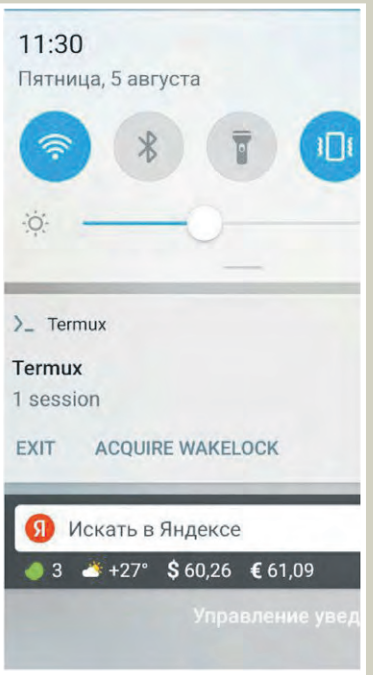
Han oppgir selv på en rekrutteringsside at han tjenestegjorde som dataanalytiker i det russiske forsvarsdepartementet i over fem år – fram til han var ferdig i mars i fjor. Også en av de arresterte i Revil-saken har ifølge russiske medier flere år bak seg i det russiske forsvaret – og utdannelse fra russisk militærakademi.

Heller ikke han har svart på Dagbladets henvendelser.

PS: Conti, gruppa med forbindelser til russisk etterretning og to antatte medlemmer med militær erfaring, angrep i mars et norsk selskap med forbindelser til forsvarssektoren i Norge. Imenco leverer utstyr til norske jagerfly og missiler, og ble hacket av Conti 28. mars. Rune Bringedal, daglig leder i Imenco, har understreket overfor Dagbladet og Kommunal Rapport at militær-relaterte opplysninger ikke kom på avveie.

PPS: Telefonnummeret til restauranten i St. Petersburg er dødt. I det russiske selskapsregisteret står det at restauranten er lagt ut for salg.

PÅ FARTEN: **På dette bildet framstår det som den antatte Conti-hackeren «Wazawaka» sitter i en svært luksuriøs flykabin. Foto: Privat**



TERMUX: **Her logger Killnet-hackeren inn, hevder han overfor Dagbladet. Han har selv sendt bilde av telefonen sin.**

EKSPERT: – FOR DÅRLIG BAKGRUNNSSJEKK

I sin åpne trusselvurdering for 2022 advarer PST mot hackergrupper som Revil og Conti:

– Norske bedrifter og offentlige virksomheter vil bli utsatt for løsepengevirus. Det er forventet at virksomheter med samfunnskritiske funksjoner vil bli rammet. Espen Johansen, CSO i det norske teknologiselskapet Visma, følger hackermiljøet tett. Han sier Contis vei fra kriminell aktør til å samarbeide tettere med en nasjonalstat – Russland – ikke er unik. Men at den er interessant.

– Contis proklamasjon og seinere fall er et eksempel på dette, sier Johansen.

Han henviser til Dagbladets avsløringer av en annen hackergruppe – Killnet – som åpent har erklært seg som en del av «Russlands cyberhær».

– Killnet har tydeligvis vært litt bedre i sine ansettelsesprosesser og bakgrunnssjekker. Conti ble som kjent «doxet» [utsatt for lekkasje] av sine ukrainske ansatte. De var naturlig nok ikke helt enig i den nye strategien.

Sikkerhetsselskapet SOC Radar mener Conti-lekkasjen viser at gruppa er sammensatt av folk fra ulike religiøse og etniske bakgrunner – og ikke er en så homogen gruppe som tidligere antatt.

Det samme het det i en uttalelse fra en annen beryktet hackergruppe – Lockbit. Etter at Conti erklærte støtte til Russland, uttalte Lockbit at gruppa inneholdt folk fra både Ukraina, Russland, Kina og USA.

– Det som er viktig for oss, er business. Vi er en apolitisk aktør. Vi bryr oss bare om penger.