Polisen

Protokollbilaga

Arkiv/Åkl. ex

Åklnr
AM-97082-21

Signerat av
Kristin Ung

Signeringsdatum
2022-05-20 11:13

Enhet
Region Mitt, Grova brott 1 PO Gävleborg

Handläggare (Protokollförare)
Kristin Ung

Datum
2022-03-18

Bitr. handläggare
Mikael Lindberg
Anders Norberg
Johan Bast

Undersökningsledare
Anna Stråth

Polisens diarienummer
5000-K753871-21

Personer i ärendet

Förtursmål	Beslag	Målsägande vill bli underrättad om tidpunkt för huvudförhandlingen
Nej		Nej
Ersättningsyrkanden		Tolk krävs

Misstänkt (Efternamn och förnamn)	Personnummer
Amin, Kojar	19970905-8490

Delgiven information om förenklad delgivning vid ett personligt möte genom att skriftlig information överlämnats

Underrättelse om utredning enligt RB 23:18a Underrättelsesätt, misstänkt	Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
Försvarare Rydin, Filip, förordnad 2021-06-07			

Underrättelsesätt, försvarare	Resultat av underrättelse mt	Resultat av underrättelse försv

Misstänkt (Efternamn och förnamn)	Personnummer
Dawlatzai, Naser Musa	19980420-8230

Delgiven information om förenklad delgivning vid ett personligt möte genom att skriftlig information överlämnats

Underrättelse om utredning enligt RB 23:18a Underrättelsesätt, misstänkt	Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
Försvarare Granfelt, Jonas, förordnad 2021-07-09			

Underrättelsesätt, försvarare	Resultat av underrättelse mt	Resultat av underrättelse försv

Notering

Innehållsförteckning

Polisen

PM

Datum
2021-11-16

Diarienr (åberopas)
5800-128/2020

Polismyndigheten
Nationella operativa avdelningen

Anom

Inledning

Svensk polis har sedan hösten 2020 medverkat i ett internationellt samarbete där vi fått möjlighet att ta del av information från en krypterad kommunikationstjänst.

Den information som lämnats till svensk polis har hanterats av underrättelseenheten vid Nationella operativa avdelningen (NOA).

Bakgrund

Under de senaste åren har krypterade kommunikationstjänster såsom EncroChat och Sky ECC använts som medel för att kommunicera i kriminella syften. Båda har numera upphört att fungera. Parallellt med dessa tjänster har det uppstått en efterfrågan för ett motsvarande system inom den grova organiserade brottsligheten.

FBI har sedan 2019 utvecklat ett krypterat kommunikationssystem som kallas ”ANOM”. Detta har marknadsförts mot kriminella organisationer som ett ”nytt sofistikerat system med enheter som var omöjliga att dekryptera av rättsväsendet”.

I praktiken var dock systemet uppbyggt på ett sätt som gjorde att alla meddelanden som skickades kunde dekrypteras av FBI. En kopia av alla meddelanden har tillgängliggjorts för FBI via en server i tredje land.

Sedan oktober 2019 har FBI och en arbetsgrupp som arbetar med brottsbekämpning på Europol tagit del av meddelanden i systemet. Kommunikationen innehåller meddelanden, fotografier, videoljud, och annan digital information

Varje användare har tilldelats ett unikt ID (Jabber Identification) som inte kan ändras. FBI har en lista över alla JID-nr, både aktiva och inaktiverade.

Kommunikationstjänsten har primärt använts av ledande personer i kriminella organisationer för att samordna narkotikahantering och penningtvätt i ett flertal länder.

Svensk polis har löpande fått ta del av kommunikationen mellan enheter som kunnat knytas till svenska användare i underrättelsesyfte men inte fått använda informationen för brottsutredning.

Avslut

Under våren 2021 startades en operation vid Europol där ett antal länder samverkat runt den tillgängliga informationen från plattformen.

Svensk åklagare har skickat framställningar om rättslig hjälp till USA innehållande begäran om att få använda materialet i svenska förundersökningar.

Informationsinsamlingen avslutades den 7 juni 2021. Detta genom att den tekniska lösningen togs ner och enheterna kan inte längre kommunicera på plattformen.

Sammanfattning gällande kommunikationstjänsten ANØM

1 Inledning

Det här dokumentet sammanfattar ett antal punkter i bilaga A i dokumentet *Teknisk information om Operation Trojan Shield* gällande den krypterade kommunikationstjänsten ANØM. Hela dokumentet finns bifogat i utredningen.

2 Teknisk beskrivning

2.1 Kryptering

Kommunikationsnätverket ANØM ger end-to-end-kryptering av meddelanden i ett slutet nätverk mellan ANØM-användare. Att nätverket är slutet innebär att den end-to-endkrypterade kommunikationen bara kan ske mellan ANØM-användare. Det är en pre-numerationsbaserad tjänst som kräver att man köper smartphones som är särskilt konfigurerade att kommunicera på ANØM, och bara telefoner som har konfigurerats på rätt sätt kan användas för kommunikationen[1]

2.2 Jabber identifier (JID)

Varje användare i ANØM identifieras med en unik identifierare (användar-ID), som tekniskt kallas för en Jabber Identifier (JID). Från början hade detta användar-ID formen av 6 alfanumeriska tecken (till exempel ”aab2c3”) och det genererades automatiskt från enhetens IMEI-nummer (International Mobile Equipment Identity number).

På grund av förändringar i operativsystemet Android gick det från december 2020 inte längre att använda IMEI-numret till att automatiskt generera användar-ID. Formatet på användar-ID ändrades därför så att det genererades automatiskt i portalen. I den här processen består användar-ID av två slumpmässigt valda ord på engelska som satts samman. ”LITTLE” och ”FISH” skulle t.ex. ge användar-ID:t ”LITTLEFISH”.[2]

2.3 Användarens visningsnamn / Alias

Enhetens användare kunde ange ett ”visningsnamn” (som också kallas smeknamn eller alias), som kunde ändras när användaren ville. Det förändrade inte deras användar-ID på

[1] Dokument: *Teknisk information om Operation Trojan Shield, sid 42, A.3.11*
[2] Dokument: *Teknisk information om Operation Trojan Shield, sid 43, A.3.18 och A.4.23*

plattformen. Det här liknar ”Från”-namnet som visas i e-postmeddelanden, som normalt skiljer sig från e-postadressen som ofta är användarnamnet.[3]

2.4 Meddelanden

En användare kan skicka ett end-to-end-krypterat meddelande till en annan ANØM-användare, förutsatt att de känner till mottagarens användar-ID.

En användare kan också skicka end-to-end-krypterade meddelanden till en grupp av ANØM-användare, och varje användare i den gruppen kan se de andra medlemmarna i gruppen. Gruppen kan ha en etikett som fungerar som ett namn på gruppen och som kan anges av gruppadministratören – normalt den som skapade gruppen – eller andra medlemmar som har fått administratörsbehörigheter för gruppen. Det här fungerar på ett liknande sätt som gruppchattar i andra meddelandeapplikationer som WhatsApp, Signal, Telegram och Facebook Messenger.

Ett meddelande, antingen till en enda användare eller till en grupp av användare, kan bestå av ett textmeddelande, en bild (t.ex. ett foto som togs med kameran på enheten), en video som spelats in med kameran på enheten, ett kort röstmeddelande (PTT – push-to-talk) eller en anteckning från enhetens valv.

Det går att citera ett meddelande genom att välja det i en konversation och trycka på svara-knappen, eller vidarebefordra det till andra mottagare genom att välja det och trycka på dela-knappen. När det görs kan deltagarna i konversationen visuellt se att meddelandet har citerats eller vidarebefordrats eftersom det visas som ett citerat block i det skickade meddelandet.[4]

[3] Dokument: *Teknisk information Operation Trojan Shield sid 48, A.7.1.2*
[4] Dokument: *Teknisk information Operation Trojan Shield sid 48, A.7.1.4.50-52 och sid 49, A.7.1.4.54*

Översättning från engelska språket

AO 106A (08/18) Ansökan om tillstånd för husrannsakan via telefon eller på annan tillförlitlig elektronisk väg

UNITED STATES DISTRICT COURT

for the

Southern District of California

sekretessen upphör 210607 enligt beslut -dig

I ärende rörande genomsökning av

(Beskriv kortfattat den egendom som ska genomsökas eller identifiera personen med namn och adress)

Ärende nr ’21 MJO1948

Google LLC
1600 Amphiteater Parkway, Mountain View,
CA 94043
Värd för expliamdavis@gmail.com

ANSÖKAN OM TILLSTÅND FÖR HUSRANNSAKAN VIA TELEFON ELLER PÅ ANNAN TILLFÖRLITLIG ELEKTRONISK VÄG

Undertecknad person som är federal polistjänsteman eller statlig åklagare, ansöker härmed om tillstånd för husrannsakan och försäkrar under ed att jag har skäl att anta att följande person eller egendom *(ange den person eller beskriv den egendom som ska sökas igenom och var den finns):*

Se bilaga A, som införlivas i denna ansökan genom hänvisning.

belägen i Northern District of California, där följande hålls gömt *(ange den person eller beskriv den egendom som ska sökas igenom):*

Se bilaga B, som införlivas i denna ansökan genom hänvisning.

Grunden för husrannsakan enligt 41 c § federala straffprocesslagen är *(kryssa för en eller flera):*

- ✓ bevis på brott
- ✓ smuggling, vinning av brott eller andra föremål som olagligen innehas

Husrannsakan har anknytning till brott mot:

Lagrum	*Beskrivning av brottet*
USC avdelning 21, 841, 846 §§	Samverkan för att distribuera kontrollerade ämnen

Ansökan bygger på följande faktiska omständigheter:
Se bifogad försäkran under ed av FBI-utredare Nicholas Cheviron, som införlivas i denna ansökan genom hänvisning

- ✓ Fortsättning på bifogat blad.

[Namnteckning]
Sökandens underskrift

Nicholas Cheviron; FBI-utredare
Namnförtydligande och titel

Intygat av sökanden i enlighet med kraven i 4.1 § federala straffprocesslagen via telefon *(ange tillförlitligt elektroniskt medel)*

Datum: 17 maj 2021

[Namnteckning]
Domarens underskrift

Stad och delstat: San Diego, Kalifornien

Michael S. Berg, federal domare
Namnförtydligande och titel

Översättning från engelska språket

FÖRSÄKRAN UNDER ED TILL STÖD FÖR ANSÖKAN OM HUSRANNSAKAN

Jag Nicholas I. Cheviron, som avlagt föreskriven ed, försäkrar härmed följande:

1. Denna försäkran under ed avges till stöd för en ansökan från Amerikas förenta stater om husrannsakan hos Google LLC på 1600 Amphitheatre Parkway, Mountain View, CA 94043, enligt beskrivningen i bilaga A, för att genomsöka följande e-postkonto:

expliamdavis@gmail.com

(nedan kallat det ifrågavarande kontot) mellan den 1 januari 2021 och den 17 maj 2021, för att klarlägga om där finns innehåll som utgör bevis, vinning av eller medel för brott mot federal lag, närmare bestämt United States Code, avdelning 21, 841 a.1, 846 §§ (samverkan för att distribuera kontrollerade ämnen), som beskrivs i bilaga B. Denna försäkran under ed och ansökan görs med stöd av 41 § federala straffprocesslagen och U.S.C. 2703 § a och b, vilka är tillämpliga på företag som tillhandahåller elektroniska kommunikationstjänster och fjärrbearbetningstjänster.

2. De faktiska omständigheter som beskrivs i denna försäkran bygger på uppgifter jag själv har kännedom om. Jag har inhämtat dessa uppgifter från andra personer under den tid jag medverkat i utredningen, däribland andra poliser, förhör med målsäganden, min genomgång av handlingar och dataregister med anknytning till utredningen, kontakter med andra personer som har personlig kännedom om de händelser och omständigheter som beskrivs här samt information som jag fått under min utbildning och yrkesutövning. Eftersom denna försäkran endast avges för att styrka att det föreligger skälig misstanke som grund för en husrannsakan, innehåller den inte alla faktiska omständigheter som jag eller andra har fått kännedom om under utredningens gång. Alla datum, klockslag och belopp som anges i denna försäkran är ungefärliga.

Översättning från engelska språket

YRKESERFARENHET OCH UTBILDNING

3. Jag är utredare (Special Agent; SA) vid Federal Bureau of Investigation (FBI) och jag har varit anställd där sedan januari 2007. Jag är för närvarande stationerad i San Diego och tillhör den grupp som arbetar med organiserad brottslighet. Innan jag började vid FBI arbetade jag som polis vid polismyndigheten i Bloomington i Illinois i ungefär tre år. Jag genomgick en grundläggande tolvveckors utbildning i narkotikabrottsbekämpning vid Illinoispolisens utbildningsinstitut i Champaign i Illinois. Under tiden jag arbetade som polis fick jag ett antal timmars specialutbildning i narkotikabrottsbekämpning. Jag fick även möjlighet att utreda och medverka i flera narkotikabrottsutredningar. Förutom den utbildning jag fått som polis har jag även genomgått en 21 veckor lång utredningsutbildning vid FBI:s akademi i Quantico i Virginia.

4. Sedan jag blev utredare vid FBI har jag utrett kriminella organisationer som bland annat ägnat sig åt narkotikahandel, penningtvätt och olaglig spelverksamhet. Jag har förhört och varit ansvarig för informatörer, gjort husrannsakningar, gripit och förhört personer, bedrivit spaning, använt elektronisk övervakning och kameraövervakning samt vittnat i federala domstolar och delstatsdomstolar. Jag har lett och medverkat i utredningar som innefattat användning av elektronisk övervakningsteknik, bland annat avlyssning godkänd av domstol, kameraövervakning, GPS-spårare och kroppsburen övervakningsutrustning. Dessa utredningar har bland annat handlat om brott enligt avdelning 18, 21, 31 and 49 i United States Code, samt brott enligt kaliforniska delstatslagar. I samband med dessa utredningar har jag gått igenom konversationer från hundratals personer som medverkat i narkotikahandel och tvättning av vinning av brott. Genom min utbildning och min yrkesverksamhet har jag skaffat mig kunskap om den teknik och de metoder som kriminella organisationer använder sig av.

Översättning från engelska språket

5. Jag har lett och medverkat i utredningar som rört identifiering av personer som medverkat i brott, där vi använt oss av telefontrafikuppgifter och telefonräkningar, ekonomiska dokument, ”liggare” (drug ledgers), fotografier och andra dokument. Jag har också medverkat i och lett utfrågningar av personer som gripits och senare samarbetat med polisen. Jag har lett och medverkat i utredningar där vi använt avlyssning av kommunikation godkänd av domstol eller andra elektroniska övervakningsverktyg. Jag har medverkat i sådana sammanhang bland annat genom att författa försäkringar under ed enligt avdelning III och söka tillstånd för husrannsakningar avseende e-postkonton och GPS-data i mobiltelefoner som byggt på information som framkommit vid avlyssning enligt avdelning III. Jag har bistått vid övervakning, granskat avlyssnad kommunikation och upprättat skriftliga rapporter baserade på mina iakttagelser.

6. Genom min utbildning och min yrkesverksamhet har jag fått kunskap om vilka metoder som narkotikasmugglingsorganisationer använder sig av, däribland metoder för distribution, lagring och transport av narkotika, metoder för att kassera in inkomster från narkotikaförsäljning och metoder för att tvätta pengar för att dölja var inkomsterna kommer från. Under den tid jag varit anställd här har jag även fått kunskap om den sedvanliga betydelsen av narkotikaslang och jargong, förpackningsmetoder samt användning och överlåtelser av kontrollerade ämnen. Jag har även kunskap om de metoder och den teknik som används av de som handlar med kokain, metamfetamin, heroin, fentanyl och marijuana.

7. Utöver den ovan beskrivna utbildningen och yrkesverksamheten har jag samarbetat med och konsulterat ett stort antal utredare och poliser som har utrett kriminella organisationer runt om i USA, däribland i södra Kalifornien, och grupper som ägnar sig åt gränsöverskridande organiserad brottslighet. Jag har även genomgått utbildning inriktad på kriminella företag och taktik som används av företag för att generera och främja olagliga medel. Denna taktik innefattar

narkotikahandel, olaglig spelverksamhet och bestickning. Jag har även genomgått utbildning inriktad på tvätt av vinning av brott. Dessutom har jag deltagit i ett stort antal arbetsgruppsmöten som rört gränsöverskridande organiserad brottslighet och olika metoder som används för att främja gränsöverskridande organiserad brottslighet. Utöver den formella utbildningen har jag rådfrågat erfarna poliser som har utbildning inom de ovannämnda områdena. Jag har även haft en stor mängd diskussioner med erfarna poliser och utredare som är specialiserade på organisationer som smugglar narkotika till sjöss eller med flyg. Tack vare dessa utredningar och utbildningar har jag fått kunskap om den verksamhet som narkotikahandels- och penningtvättsorganisationer bedriver i och utanför USA.

8. Min erfarenhet som polis och som utredare hos FBI, min medverkan i en rad utredningar om kriminella organisationer, mina samtal med andra utredare vid FBI och vid USA:s federala narkotikapolismyndighet (Drug Enforcement Administration; DEA) och andra poliser som har kunskap om narkotikahandel, penningtvätt och gränsöverskridande organiserad brottslighet, utgör grunden för nedanstående utlåtanden och slutsatser, som bygger på de faktiska omständigheter som beskrivs här.

SKÄLIG MISSTANKE

A. Bakgrund till den kriminella användningen av krypterade enheter

9. År 2017 började FBI i San Diego att utreda ett företag som hette Phantom Secure och som tillhandahöll krypterade enheter.[1] Utredningen visade att Phantom Secure enbart sålde sina krypterade enheter till personer som

[1] En ”krypterad enhet” är en enhet för kommunikation som (1) skickar och tar emot krypterad elektronisk kommunikation och/eller (2) krypterar data som lagras i enheten. Liksom var fallet med andra konkurrerande fabrikat hade Phantom Secures enheter ett begränsat användningsområde. De kunde inte användas för att ringa ett vanligt telefonsamtal eller surfa på internet. Phantom Secure tillhandahöll serviceplaner för kryptering som omfattade 2–6 månader och enheterna kostade mellan USD 1 500 och USD 2 000 styck för en sexmånaders serviceplan. Enheterna kunde inte köpas i vanliga butiker eller på internet. Den som var intresserad av att använda sig av en sådan enhet måste ha kontakter med en känd distributör, bara för att få möjlighet till ett inledande samtal för att köpa en enhet. Phantom Secures enheter användes inom en sluten krets. Det innebar att kommunikationen mellan olika enheter var begränsad till en sluten grupp av personer som man själv valt ut och som bara använde andra enheter från Phantom Secure.

tillhörde kriminella organisationer. Företaget vände sig till kunder i gränsöverskridande brottsorganisationer (i första hand narkotikahandlare) och tillhandahöll en uppsättning tjänster som var avsedda att hindra polisen från att på laglig väg kunna övervaka deras kommunikation och inhämta bevis på brottslig verksamhet. Utredningen visade att Phantom Secures enheter användes av kriminella organisationer runt om i världen.

10. I mars 2018 röstade en åtalsjury i Southern District of California för ett åtal mot Phantom Secures VD Vincent Ramos och fyra andra chefer i företaget. Åtalet avsåg brott mot RICO och medverkan till distribution av kokain. Ramos greps i mars 2018.[2] Den 2 oktober 2018 erkände Ramos de brott han åtalats för. Under den förhandling som hölls i samband med detta medgav Ramos att Phantom Secure (1) hade medverkat i införsel, utförsel och distribution av narkotika runt om i världen, (2) förhindrat utredningen genom att förstöra och undanhålla bevis från polisen och (3) tvättat vinning av narkotikahandel. Ramos dömdes till nio års fängelse och tillgångar till ett värde av USD 80 000 000,00 som utgjorde vinning av denna brottsliga verksamhet förverkades.

11. Eftersom krypterade enheter ger ett ogenomträngligt skydd mot polisens övervakning och brottsbekämpning, finns det en stor efterfrågan på dessa tjänster bland gränsöverskridande kriminella organisationer. Det finns andra företag än Phantom Secure på marknaden som också tillhandahåller krypterade kommunikationstjänster och de fortsätter att blomstra. Genom min utbildning och min yrkesverksamhet är jag medveten om att det fortfarande finns en stor efterfrågan på sådana krypterade kommunikationsplattformar bland kriminella. Det beror framför allt på att det bland grupper som ägnar sig åt organiserad brottslighet, särskilt gränsöverskridande sådan, finns ett behov av en pålitlig kommunikationsmetod som de bedömer säker och omöjlig för polisen att

[2] Gripandet av Ramos ledde till att Phantom Secure lades ned. Sedan gripandet av Ramos har FBI inte funnit en enda Phantom Service-användare som inte varit kriminell. FBI gav alla som använde en enhet från Phantom Secure möjlighet att träda fram och hämta fram deras uppgifter. Ingen av Phantom Secures användare framställde någon sådan begäran till FBI.

övervaka och avlyssna. Gränsöverskridande brottsliga organisationer utgör målgruppen för denna teknik, eftersom det är en förutsättning för att de ska kunna bedriva sin brottsliga verksamhet att polisen inte kan avslöja dem. I synnerhet narkotikahandel bygger på internationell samordning i realtid mellan olika aktörer. De höga olagliga intäkterna från den internationella narkotikahandeln innebär att kriminella både är beredda och har råd att betala USD 2 000 för en enhet som bara har en enda funktion: att skicka säkra, krypterade meddelanden – inom en sluten krets. Utredningen kring Phantom Secure visade att krypterade enheter inte brukar användas av personer som värnar om sin integritet, eftersom de har en begränsad funktion och är dyra.

B. En hemlig informatör gav FBI insyn i ett företag som höll på att utveckla en krypterad kommunikationstjänst

12. Efter att Ramos hade gripits rekryterade FBI i San Diego en hemlig informatör[3] som hade arbetat med att utveckla en krypterad kommunikationsprodukt i ”nästa generation”, som var tänkt att konkurrera om marknadsandelar med etablerade företag som tillhandahöll krypterade enheter. Det tomrum som uppstod när Phantom Secure avvecklades gav kriminella användare tillfälle att byta till ett nytt säkert fabrikat. Informatören hade tidigare distribuerat Phantom Secures och Sky Globals[4] plattformar till gränsöverskridande kriminella organisationer och investerat betydande belopp i att utveckla en ny krypterad kommunikationsplattform. Informatören erbjöd FBI att använda denna nya plattform, kallad ”Anom”, i pågående och kommande utredningar. Informatören gick även med på att distribuera Anom-enheter till

[3] Den hemliga informatören hade arbetat för FBI-utredare sedan 2018 i utbyte mot en möjlighet till nedsatt straff för brott som informatören stod åtalad för. Informatören hade fått USD 120 000 från FBI för sina tjänster och USD 59 508 som ersättning för kostnader för boende och resor. Den information och de tjänster som informatören har tillhandahållit i det här fallet anses tillförlitliga, eftersom de delvis har bekräftats av registrerade meddelanden, förhör och affärshandlingar. Informatören har tidigare dömts till sex års fängelse för införsel av narkotika.

[4] Den 12 mars 2021 röstade en åtalsjury i Southern District of California för ett åtal mot Sky Globals VD Jean Francois EAP och en av Skys distributörer, Thomas Herdman. Åtalet avsåg medverkan till brott mot RICO och byggde på medverkan i narkotikahandel och försvårande av utredningen. Offentliggörandet av åtalen och husrannsakningarna vid Sky Globals infrastruktur medförde att Sky Globals verksamhet upphörde.

vissa personer i dennes befintliga nätverk av distributörer av krypterade kommunikationsplattformar, av vilka alla har direkta kopplingar till gränsöverskridande kriminella organisationer. Eftersom syftet med krypterade kommunikationsplattformar är att undgå lagföring, bygger distributionen av dessa på förtroende. Detta ljusskygga distributionssystem är delvis avsett att hindra polisen från att komma åt innehållet i enheterna. Phantom Sercure-utredningen visade att distributörerna måste granska presumtiva köpare för att förhindra att polisen fick tillgång till dessa enheter. Granskningsprocessen bygger på att det antingen finns en personlig relation eller på att köparen har skaffat sig ett rykte som bygger på tidigare eller pågående brottsligt samröre. Genom att presentera Anom för informatörens betrodda distributörer, som även kriminella organisationer litade på, ville FBI öka användningen av Anom inom dessa nätverk.

13. FBI inledde en ny hemlig utredning, Operation Trojan Shield, vilken inriktades på att använda Anom genom att introducera tjänsten för kriminella närverk och samarbeta med internationella samarbetspartners, däribland Australiens federala polis (AFP), för att övervaka kommunikationen. Innan tjänsten kunde tas i bruk byggde emellertid FBI, AFP och informatören in en huvudnyckel i det befintliga krypteringssystemet som i hemlighet fogas till varje meddelande och gör det möjligt för polisen att dekryptera och lagra meddelandet när det överförs. Anom-användarna kände inte till denna möjlighet. När det gäller enheter som finns utanför USA,[5] sänds inom ramen för Trojan Shield-utredningen en krypterad dold kopia av meddelandet till en ”iBot-server” som finns utanför USA, där den dekrypteras från informatörens krypteringsnyckel och därefter omedelbart återkrypteras med FBI:s krypteringsnyckel. Det återkrypterade meddelandet flyttas därefter till en andra FBI-ägd iBot-server, där det dekrypteras och dess innehåll blir tillgängligt för en första granskning.

[5] Såsom förklaras vidare nedan, fångas enheter som finns i USA inte upp av den andra FBI-ägda servern, eftersom USA är avgränsat med geostaket (geofence).

Översättning från engelska språket

14. Varje Anom-användare tilldelas en viss Jabber-identitet (”JID”) av informatören eller av en Anom-administratör. En JID liknar en ”PIN” i Blackberry Messenger. En JID är antingen en bestämd unik alfanumerisk identitet eller, när det gäller nyare enheter, en kombination av två engelska ord. Anom-användare kan välja sina egna användarnamn och ändra sin lista över användarnamn senare. Inom ramen för Trojan Shield-utredningen har FBI en lista över olika JID och motsvarande användarnamn för Anom-användare.

C. Den hemliga informatörens kriminella distributörer tillhandahåller bara Anom-enheter åt transnationella brottsorganisationer

15. Informatören har kontrollerat distributionen av Anom-enheter i samråd med FBI. I oktober 2018 började informatören erbjuda dessa enheter till tre tidigare Phantom-distributörer med kopplingar till kriminella organisationer, främst i Australien. Dessa tre personer, som utnyttjade sina erfarenheter som Phantom-distributörer och som såg möjligheter till stora inkomster, tackade ja till erbjudandet. För detta inledande ”betatest” fick AFP tillstånd av domstol att övervaka Anom-enheter tillhörande personer som befann sig i eller hade en tydlig anknytning till Australien. Omkring femtio enheter distribuerades som en del av betatestet och det blev lyckat. Tack vare övervakningen av denna kommunikation kunde AFP få insyn i två av de mest sofistikerade kriminella nätverken i Australien. AFP har lämnat allmänna upplysningar till FBI i San Diego om vilken typ av samtal som förs via Anom.[6] Det innefattar narkotikahandel (bland annat diskussioner om transport av hundratals kilo narkotika), vapenköp och annan olaglig verksamhet. Precis som FBI hade konstaterat när det gällde Phantom Secure, använde 100 procent av användarna Anom för brottslig verksamhet, enligt den australiska polisen. Övervakade konversationer har också visat att personer inom gränsöverskridande kriminella

[6] Den australiensiska domstolens beslut att godkänna övervakning av Anom-kommunikation medgav inte att man delade med sig av innehållet till utländska samarbetspartners.

organisationer har velat förse högt uppsatta personer i kriminella nätverk utanför Australien med dessa enheter.

16. Antalet enheter i Australien ökade till att börja med långsamt, men ökningstakten blev successivt snabbare när ryktet spreds av informatörens kriminella distributörer och andra slutanvändare. Spridningen sköt fart under sommaren 2019. I samband med det lyckade testet i Australien, kunde informatören konstatera att efterfrågan på enheter ökade såväl inom som utanför Australien. I samarbete med FBI började informatören öka spridningen av enheter till andra kriminella affärskontakter i sitt distributionsnät. Australien fortsatte att övervaka denna kommunikation.

17. FBI granskade emellertid ännu inte själv något dekrypterat innehåll från Anoms kriminella användare. Under sommaren 2019 anlitade utredningsgruppen företrädare från ett tredjeland för att ta emot en egen iBot-server och få fram innehållet i kommunikationen mellan olika Anom-användare. Förhandlingarna om logistiken och regelverket i tredjelandet fortsatte under hösten 2019. Tredjelandet gick med på att utverka ett domstolsbeslut i enlighet med dess eget regelverk för att få kopiera av en iBot-server som var placerad där och förse FBI med en kopia, med stöd av ett avtal om ömsesidig rättslig hjälp. Till skillnad från vid det australiska betatestet, skulle tredjelandet inte granska innehållet först. FBI avgränsade USA med ett geostaket, vilket innebar att inga utgående meddelanden från en enhet med amerikansk landskod skulle ha någon kommunikation på FBI:s iBot server, men om enheter hamnade i USA gick AFP med på att övervaka dessa enheter för att se om de innehöll hot mot liv, på grundval av AFP:s normala riktlinjer och rutiner.

18. I oktober 2019 utverkade tredjelandet ett domstolsbeslut som innebar att iBot-servern fick kopieras och att dess innehåll fick tas emot varannan eller var tredje dag. Enligt det första avtalet om ömsesidig rättslig hjälp fick FBI ta emot data mellan den 7 oktober 2019 och den 7 januari 2020. På grund av tekniska problem med dekrypteringen och med att återge innehållet i ett

användbart format, började FBI inte ta emot det faktiska serverinnehållet från tredjelandet förrän den 21 oktober 2019. Det fanns då flera hundra Anom-användare, av vilka merparten fortfarande fanns i Australien. Sedan oktober 2019 har tredjelandet utverkat ytterligare ett domstolsbeslut enligt det egna landets lagar för att kopiera iBot-servern och USA har tagit emot serverdata med stöd av ytterligare avtal om ömsesidig rättslig hjälp. Tredjelandet förser FBI med Anomserverdata varje måndag, onsdag och fredag och kommer att fortsätta med det fram tills tredjelandets domstolsbeslut upphör att gälla den 7 juni 2021. Dessa data innefattar de krypterade meddelandena från alla Anom-användare med några få undantag (t.ex. meddelanden från cirka 15 Anom-användare i USA som skickas till någon annan Anom-enhet som inte granskas av FBI).

19. Sedan oktober 2019 har FBI granskat innehållet från iBot-servern i tredjelandet med stöd av avtalet om ömsesidig rättslig hjälp. Meddelandena har översatts (vid behov och när översättningar har gått att ordna) och FBI har katalogiserat mer än 20 miljoner meddelanden från sammanlagt 11 800 enheter (av vilka omkring 9 000 för närvarande är aktiva) i mer än 90 länder. Nedanstående bild visar var i världen Anomanvändarna finns:

[Bild]

De fem länder som för närvarande har flest Anom-enheter är Tyskland, Nederländerna, Spanien, Australien och Serbien.

20. Trojan Shield-utredningen har visat att Anom-enheter används av gränsöverskridande kriminella organisationer för att handla med narkotika och tvätta inkomster från narkotikaförsäljningen. Distributörerna av Anom-enheter försvårar även utredningarna genom att fjärradera innehållet i enheterna när de tas i beslag av polisen. Granskningen av Anom-meddelanden har vidare gett upphov till ett antal korruptionsutredningar på hög nivå i olika länder. De mest framträdande distributörerna utreds för närvarande av FBI för medverkan i ett företag som främjar internationell narkotikahandel, penningtvätt och försvårande av utredningar. FBI har, på senare tid med hjälp av Europols specialgrupp,

Översättning från engelska språket

identifierat mer än 300 olika gränsöverskridande kriminella organisationer som använder Anom, däribland den organiserade brottsligheten i Italien, MC-gäng och olika internationella celler för anskaffning, transport och försäljning av narkotika. Jag har granskat en del meddelanden på Anom-plattformen sedan 2019 och jag har pratat med andra FBI-utredare som har granskat innehållet. På grundval av min kännedom om FBI:s granskning av innehåll från alla internationella Anom-användare och mina erfarenheter av att utreda gränsöverskridande kriminella organisationer, är det min uppfattning att Anom-enheter enbart används för att diskutera brott öppet eller för att upprätthålla förbindelser för att främja sådana brott.

21. Trojan Shield-utredningen har visat att kriminella organisationer delar upp sin verksamhet mellan olika krypterade kommunikationstjänster. Vissa användare nyttjar till exempel olika tjänster för olika delar av en narkotikatransaktion. Jag har sett konversationer där Anom har använts för logistiken för en narkotikatransport, medan Ciphr eller Sky har använts för att koordinera döljandet av de olagliga intäkterna. Denna uppdelning visar att olika delar av branschen för krypterade kommunikationstjänster är sammanlänkade med varandra. Denna sammanlänkning blev också uppenbar när efterfrågan ökade i samband med att två stora plattformar avslöjades till följd av Trojan Shield-utredningen. Först offentliggjorde europeiska utredare en utredning av EncroChat i juli 2020 vilket ledde till att den avvecklades. Efterfrågan på Anom-enheter bland kriminella grupper ökade efter detta offentliggörande. I mars 2021 ledde vidare offentliggörandet av åtalet mot Jean Francois Eap och avvecklingen av Sky Global till en starkt ökad efterfrågan på Anom-enheter från de kriminella organisationernas sida. Innan Sky avvecklades fanns det omkring 3 000 aktiva Anom-användare. Sedan den 12 mars 2021 finns det som en direkt följd av åtalen mot Sky Global nästan 9 000 aktiva Anom-användare. Kriminella som använder sig av krypterade kommunikationstjänster är hela tiden på jakt efter nya säkra tjänster, och distributörerna av dessa tjänster har i åratal gjort det

möjligt för kriminella att kommunicera utan insyn. Ett av målen med Trojan Shield-utredningen är att rubba tilltron till hela den här branschen genom att visa FBI är villig och har förmåga att ta sig in i dessa plattformar och övervaka meddelanden.

D. Exempel på kriminella konversationer på Anom

22. Här nedan följer ett litet men representativt urval av det kriminella innehåll från utländska Anom-enheter som FBI har granskat sedan oktober 2019.

23. Den 4 januari 2020 diskuterade användaren av JID b14f2c, som med hjälp av granskningar av Anom-meddelanden har identifierats som Domenico Catanzariti, och användaren av JID 31bcf1, som har identifierats som Salvatore Lupoi, ”atlas” kokainlager. Catanzariti sa att ”allt på [batmanfotot) var atlas lager” och ”tror att han har fått in det”. Lupoi svarade: ”Du drömmer. Fattar du. Vad han erbjuder det till dig för.” Catanzariti frågade därefter vad Lupoi menade och om Atlas hade skickat samma foto där atlas sa att allt var hans. Lupoi sa att han aldrig hade fått fotot. Catanzariti svarade att det var Lupoi som hade skickat det till honom för en månad sedan. Catanzariti skickade därefter nedanstående foto på Atlas lager till Lupoi och det visade hundratals kilo kokain med batmanetiketter.

[Fotografi]

Lupoi frågade då Catanzariti vilket styckpris han säger till dem. Catanzariti föreslog 150 eller 160 (150 000–160 000 AUD/kilo). Lupoi höll med om att högst 160 var det rätta priset.

24. Den 23 mars 2020 frågade användaren av JID 58f4a9, som med hjälp av Anom-meddelanden har identifierats som Baris Tukel, användaren av JID cfdf8a, som har identifierats som Shane Geoffrey May, vilket det aktuella priset på kokain var. Tukel frågade också om May hade den där ”byggklossadressen”. May svarade att kokainet låg på omkring 200k mark och undrade om Tukel hade några nyheter. Tukel skrev: ”Ok sötnos, jag har ett litet jobb som dök upp för

Översättning från engelska språket

byggklossen” och ”det finns 2 kg som har lagts i franska diplomatiska förseglade kuvert ut från Bogotta [sic]” och ”de har redan fått in ett antal paket”. Tukel tillade: ”Enda problemet är att COL tar 50/4 partners inklusive dig kommer att behöva dela på resterande 50” (vilket betyder att de colombianska distributörerna tar 50 % av vinsten medan fyra andra personer får dela på resterande 50 %). Tukel skrev: ”De kan göra det varje vecka” (vilket betyder att paket innehållande två kilo kan skickas varje vecka). May svarade att det lät bra och att han skulle skicka adressen inom kort. Tukel skickade sedan tre foton: två på de franska diplomatiska postväskorna och ett på det kokain som fanns tillgängligt för att skicka.

[Fotografier]

Efter att han skickat fotona på kokainpaketen skrev Tukel: ”De väntar på att bli skickade från det här gänget”. Senare i konversationen tillade Tukel: ”De har redan landat de här jobben i brisbane (Australien)”.

25. Den 29 maj 2020 skrev användaren av JID c2c367, med användarnamnet ”Real G”, till användaren av JID 08511a, med användarnamnet IRONMAN: ”Sydsidan undrade vilka priser som gäller i HK (Hong Kong) per styck [kilo narkotika]? Vilken är inträdesavgiften? Och om de har någon i hamnen för att få in det? De säkerställer utförsel 90 % enbart om polisen i Bogota fått info om det då är de ovanför det. Fråga HK om de kan ta emot banan för turbo [hamnstaden Turbo, Colombia] skickar banan till HK till kommer att bli bra om möjligt eftersom det här kommer att vara slutprodukt.” IRONMAN svarade att han inte visste vilket styckpriset var i Hong Kong eftersom Hong Kong är väldigt annorlunda och sa att priset just nu för ett kilo i Australien är cirka 100 000. IRONMAN sa också att det ”inte fanns någon i hamnen som kunde få in det”, vilket betydde att de inte hade tillgång till någon korrupt tjänsteman som kunde se till att narkotikan kom in utan problem. IRONMAN frågade hur narkotikan gömdes i bananerna. Real G svarade: ”De har packat jobbet [paketen med narkotika] inuti lådorna.” Real H skickade följande foto på

paketen med narkotika (misstänkt kokain med tanke på formen och storleken) packad i ett bananparti:

[Fotografi]

Real G tillade: ”De täcker detta med ett lager bananer.” Sedan diskuterade de om man behövde skicka några lagliga partier ”eftersom ingen i HK öppnar dörren”.

26. I oktober 2020 arrangerade en gränsöverskridande brottsorganisation en transport av kokain från Ecuador till Belgien som skulle föras in med en transportcontainer dolt i tonfiskburkar. FBI granskade innehållet i meddelandena från den gränsöverskridande brottsorganisationen. Meddelandena visade att den gränsöverskridande brottsorganisationen diskuterade logistiken kring införseln och lämnade information om containern. Denna information vidarebefordrades till amerikanska myndigheter i Bryssel, som samarbetade med belgisk polis för att försöka hitta den misstänkta containern. När polisen hade letat klart hittade de omkring 613 kilo kokain. Dessutom vidarebefordrades information till polisen Ecuador där det ecuadorianska tonfiskföretaget identifierades, vilket ledde till ytterligare ett beslag av cirka 1 523 kilo kokain som placerats i en container som skulle till Antwerpen i Belgien.

[Fotografier]

27. I april 2021 arrangerade en gränsöverskridande brottsorganisation en transport av kokain (med hjälp av Anom-enheter) från Ecuador till Spanien som skulle föras in med en transportcontainer dolt i fryst fisk. FBI och den spanska polisen granskade meddelandena som innehöll närmare uppgifter om transporten och distributionen efter att narkotikan kommit till Spanien. Den misstänkta containern anlände till hamnen i Algeciras i Spanien den 29 april 2021. Spansk polis sökte igenom den och när de var klara hade de hittat omkring 1 401 kilo kokain.

[Fotografi]

Översättning från engelska språket

28. I maj 2021 arrangerade en gränsöverskridande brottsorganisation en transport av kokain (med hjälp av Anom-enheter) från Costa Rica till Spanien som skulle föras in med en transportcontainer dolt i urgröpta ananaser. FBI och den spanska polisen granskade meddelandena som innehöll närmare uppgifter om transporten och distributionen efter att narkotikan kommit till Spanien. Den misstänkta containern anlände till hamnen i Algeciras i Spanien den 12 maj 2021. Spansk polis sökte igenom containern och när de var klara hade de hittat omkring 1 595 kilo kokain.

[Fotografi]

[Fotografi]

29. De ovan återgivna konversationerna är ett litet urval av de mer än 20 miljoner meddelanden från kriminella Anom-användare som FBI har granskat. Av dessa meddelanden har mer än 450 000 foton skickats med uppgifter om konversationer på andra krypterade plattformar där man diskuterat brottslig verksamhet, transaktioner med kryptovaluta, omfattande penningsmuggling, korruption inom polisen[7] och information om självidentifiering. Ett representativt urval av foton som bland annat visar stora mängder pengar som är inkomster från olagliga transaktioner, GPS-lokalisering av narkotikatransporter och diskussioner om kriminell verksamhet på andra krypterade plattformar, har lagts in nedan:

[Fotografier]

E. Identifiering av det ifrågavarande kontot och skälig misstanke som grund för husrannsakan

30. Den 25 februari 2021 vidarebefordrade JID 11096a (med användarnamnet TOM FORD) ett meddelande från JID 700204 (med användarnamnet Sion) där det stod: ”Vi är beredda att ta emot paketet idag bro.

[7] Information som granskats på plattformen har visat att känsliga uppgifter från polisen, som rapporter och beslut, har vidarebefordrats till gränsöverskridande brottsorganisationer. Gränsöverskridande brottsorganisationer har även fått reda på planerade polisinsatser mot dem eller mot andra kriminella bundsförvanter.

Översättning från engelska språket

Säg till honom att de två adresser som är tillgängliga just nu är hotellet och den mekaniska verkstaden. Nästa mekaniska verkstad och hotell väntar jag på slutligt godkännande för att få med dem.” Sion svarade: ”Jag förstår bror, men jag kan inte skicka på dessa två adresser nu, eftersom det kommer att bli fler paket att skicka till samma adress.” ”Jag kan skicka till samma adress en gång i veckan, på så sätt blir det säkert”, ”6 kg”, och ”om jag får fler adresser kan jag skicka fler KGS”. TOM FORD svarade: ”Ok broder vi kommer att ha det oroa dig inte.” Sion svarade: ”Tack broder, låt oss börja arbeta med fler KGS broder.”

31. Senare i samma konversation skickade TOM FORD TVÅ fotografier på en faktura till Sion. Fakturan uppgavs avse en ”sittkista” som skickats från ”Liam Davis” med adressen: Lowe’s Home Improvement på 2515 Palomar Airport Road, Carlsbad, CA 92008, USA, telefonnummer 760-331-0195 och e-postadress expliamdavis@gmail.com (det ifrågavarande kontot). Jag är medveten om att detta är den rätta adressen och det rätta telefonnumret till en Lowe’s-butik i Carlsbad (som ligger i Southern District of California). Enligt Anoms registrerade metadata vid tidpunkten för den här konversationen, befann sig TOM FORD sannolikt i Australien och Sion i Armenien.

[Fotografier]

32. Mottagaren av leveransen var ”Pro Worx Performance” på 288 Princes Hwy, Banksia NSW 2216, Australien med telefonnummer +61 403 305 460. Av offentliga register framgår att det finns en mekanisk verkstad som heter Pro Worx Performance på 28**6** Princes Hwy med samma telefonnummer som det som angavs i mottagaruppgifterna.

33. Efter att TOM FORD hade skickat dessa foton, uttryckte Sion lättnad: ”eftersom paketet är klart så vill jag skicka det idag, jag har beställt nästa KG för att förbereda avsändande.” I samma meddelandetråd skickade TOM FORD och Sion foton på kokainblock till varandra och hävdade att det var från Amerika och på väg till Europa.

[Fotografi]

Översättning från engelska språket

34. På grundval av innehållet i dessa konversationer och min kunskap om hur Anom-enheter brukar användas, är min uppfattning att TOM FORD och Sion samordnade leveransen av sannolikt sex kilo kokain från Carlsbad till Australien i februari 2021. Jag tror också att de diskuterade ytterligare transaktioner så snart fler leveransadresser i Australien kunde ordnas.

35. På grundval av ovanstående diskussioner och andra konversationer som jag har granskat, är det min uppfattning att denna gränsöverskridande brottsorganisation där TOM FORD och Sion ingår, använder sig av leveransuppgifter från verkliga företag för att dölja narkotikatransporter. Min uppfattning är att gruppen kommer att fortsätta att använda sig av e-postkonton, däribland det ifrågavarande kontot, för att skicka fakturor, uppgifter om konossement och transportuppgifter och fortsätta att främja narkotikatransaktioner. Den gränsöverskridande brottsorganisationen har särskilt använt sig av det ifrågavarande kontot vid åtminstone en transport av en misstänkt kokaintransaktion från Carlsbad i Kalifornien till Australien. E-postkontot innehåller sannolikt bevis på den gränsöverskridande brottsorganisationens tidigare narkotikasmugglingsverksamhet och det kan vara till hjälp för att identifiera framtida transporter och de personer som använder det ifrågavarande kontot, som medverkar i distribution av kontrollerade ämnen.

36. Jag begär härmed tillstånd för att inhämta innehållet på det ifrågavarande kontot mellan den 1 januari 2021 och den 17 maj 2021, eftersom narkotikasmugglingsuppdraget i fråga diskuterades första gången i februari 2021 och det finns skäl att anta att det kan finnas bevis från den här perioden, enligt beskrivningen i bilaga B. Genom min utbildning och min erfarenhet vet jag att det kan ta många månader att genomföra metoder för att dölja narkotika. Jag vet också att man ofta prövar att göra flera ”testsändningar” innan man faktiskt skickar narkotika och att de också kräver användning av e-postkorrespondens för att arrangera och använda som bevis på transporttransaktionen. Genom dessa ”testständningar” kan man övervaka hur lång tid en transport tar, om det finns

Översättning från engelska språket

några problem i tullen i utförsel- eller införsellandet och huruvida transportkanalerna fungerar. Det kan alltså finnas bevis på planering och förberedelser på det ifrågavarande kontot under flera månader innan ett verkligt narkotikaparti skickas iväg. Jag begär också tillstånd för att söka igenom det ifrågavarande kontot mellan den 1 januari 2021 och den 17 maj 2021, eftersom TOM FORD och Sion anspelade på fler transporter i framtiden med kilovis med narkotika. På grundval av deras konversationer via Anom, är det min uppfattning att de eller deras kumpaner kan ha fortsatt att använda det ifrågavarande kontot för framtida narkotikatransaktioner.

GRUNDER FÖR DEN BEVISNING SOM KAN FÅS FRAM GENOM HUSRANNSAKAN

37. Mot bakgrund av min utbildning och erfarenhet, samråd med andra poliser som har erfarenhet av att utreda internationell narkotikasmuggling till sjöss och alla de omständigheter och uppfattningar som beskrivs i denna edliga försäkran, anser jag att det finns sannolika skäl att misstänka att det ifrågavarande kontot används för att dölja distribution av kontrollerade ämnen på fartyg och att följande bevisning kan finnas lagrad hos Google LLC med avseende på det ifrågavarande kontot:

a. Meddelanden, redogörelser och bilagor som syftar till att diskutera eller fastställa skapandet av företag, register, fakturor, transaktioner, uppgifter om konossement, transportuppgifter för att dölja distribution av kontrollerade ämnen eller för att göra testsändningar.

b. Meddelanden, redogörelser och bilagor som syftar till att diskutera den lagliga lasten eller uppgifter om transportmedel som används för att dölja distribution av narkotika eller gör att göra testsändningar.

c. Meddelanden, redogörelser och bilagor som syftar till att identifiera personer eller platser som utgör källan till den dolda narkotikan samt mottagarpersoner och platser och hamnar för den dolda narkotikan.

d. Meddelanden, redogörelser och bilagor som syftar till att identifiera användarna av användarnamnen TOM FORD, Sion och eventuella kumpaner till dem (som Liam Davis) som är inblandade i aktiviteterna i punkt III a–c ovan.

e. Meddelanden, redogörelser och bilagor som ger ett sammanhang till de ovan beskrivna meddelandena, exempelvis e-post som skickats eller tagits emot i tidsmässig närhet till relevanta e-postmeddelanden och e-postmeddelanden som syftar till att identifiera användarna av det ifrågavarande kontot.

REELL RISK FÖR ATT BEVIS FÖRSTÖRS

38. Min erfarenhet och utbildning och den erfarenhet och utbildning som andra utredare som jag har haft kontakt med har, visar att elektroniskt lagrade uppgifter kan raderas permanent eller ändras av användare som har grundläggande datakunskaper. I det här fallet är det bara om personen i fråga i förväg får en varning om detta husransakningsbeslut, som det finns en verklig risk för att bevis förstörs.

TIDIGARE FÖRSÖK ATT INHÄMTA DENNA BEVISNING

39. USA har inte försökt att få fram dessa uppgifter på något annat sätt.

TJÄNSTELEVERANTÖREN

40. Google LLC är ett internetföretag som bland annat tillhandahåller elektroniska kommunikationstjänster till sina prenumeranter. Google LLC:s e-posttjänst (Gmail) gör det möjligt för prenumeranterna att kommunicera med varandra elektroniskt via internet. ISP:s prenumeranter får tillgång till ISP:s tjänster via internet.

41. Google LLC:s prenumeranter använder användarnamn när de kommunicerar med varandra. Användarnamnet kan vara personens riktiga namn, men det behöver inte vara det. Google LLC kontrollerar inte den information som prenumeranten lämnar för att få tillgång till företagets gratistjänster.

Översättning från engelska språket

42. När man skapar ett Google-konto och varje gång man därefter går in på det, loggar Google LLC IP-adressen för den dator som används för att gå in på kontot. En IP-adress är en unik adress som används för att koppla upp en dator mot internet. IP-adresser hyrs ut till företag och privatpersoner av internetleverantörer. Genom att få fram de IP-adresser som har gått in på ett visst Google-konto kan man ofta identifiera den internetleverantör som äger och har hyrt ut den adressen till sin kund. Prenumerantinformation för den kunden kan fås fram genom ett lämpligt rättsligt förfarande.

RUTINER FÖR ELEKTRONISKT LAGARAD INFORMATION

43. Federala utredare och personal som bistår vid utredningarna har utbildning för och erfarenhet av att identifiera kommunikation som är relevant för de brott som utreds. Googles personal har inte det. Det skulle vara olämpligt och opraktiskt om federala utredare skulle söka efter relevanta konton i Googles stora datornät och sedan analysera innehållet på de kontona i Google LLC:s lokaler. Det skulle allvarligt störa Google LLC:s verksamhet.

44. Jag begär därför tillstånd att beslagta allt innehåll, inklusive e-post och bilagor, lagrade snabbmeddelanden, lagrade röstmeddelanden, fotografier och annat innehåll från Googles konto, enligt beskrivningen i bilaga B. För att uppnå målet med husrannsakan med minsta möjliga ingrepp i Google LLC:s affärsverksamhet, för att skydda integriteten för ISP-prenumeranter vars konton vi inte fått tillstånd att söka igenom och för att genomföra denna utredning på ett effektivt sätt, ansöker FBI om tillstånd att låta Google LLC ta en digital kopia av hela innehållet i det konto som ska beslagtas. Den kopian kommer att lämnas till mig eller någon annan behörig federal utredare. En kopia kommer att tas av kopian och den kommer sedan att analyseras för att identifiera kommunikation och andra elektroniska uppgifter som ska tas i beslag enligt bilaga B. Relevanta elektroniska uppgifter kommer att kopieras över till separata medier.

Översättning från engelska språket

Originalmedierna kommer att förseglas och behållas för att vid behov kunna slå fast äktheten.

45. För att kunna analysera de uppgifter som Google LLC ska tillhandahålla kan det komma att krävas särskild teknisk kompetens, utrustning och programvara. Det kan också komma att bli mycket tidskrävande. När man till exempel söker efter nyckelord ger det ofta många tusen ”träffar” och var och en av dem måste granskas i sitt sammanhang för att avgöra om uppgifterna omfattas av husrannsakan. Bara för att man får en relevant ”träff” innebär det inte att granskningsprocessen är klar. Nyckelordssökningar fångar inte upp felstavade ord eller användning av förtäckt språkbruk eller slang. Nyckelordssökningar är också begränsade när elektroniska uppgifter är på eller använder främmande språk. Vissa filformat tillåter inte heller nyckelordssökningar. Nyckelord söker igenom text. Många vanliga e-post-, databas- eller kalkylprogram, där filer kan ha bifogats e-postmeddelanden, lagrar inte data som sökbar text. I stället lagras dessa data i ett annat proprietärt format än textformat. I takt med att tjänsteleverantörerna tillhandahåller allt större lagringsvolymer, tar det dessutom allt längre tid att ordentligt analysera hämtad data dramatiskt. Internetleverantörerna ordnar inte alltid de elektroniska filer de tillhandahåller kronologiskt, vilket innebär att granskningen blir ännu mer tidskrävande och även innebära att granskaren måste granska varje sida eller dokument för att se om den innehåller något relevant material.

46. Detta innebär att när man söker igenom hämtad data för att se om det finns information som kan tas i beslag enligt husrannsakningsbeslutet, kan det krävas en rad olika dataanalysmetoder och det kan ta veckor eller till och med månader. Nyckelorden behöver ändras fortlöpande beroende på vilka resultat man kommit fram till och beroende på hur de uppgifter som internetleverantören tillhandahåller är organiserade och vilket format och språk de har, kan granskaren behöva granska varje uppgift för att avgöra om den motsvarar bilaga

Översättning från engelska språket

B. Den personal som utför granskningen kommer att avsluta analysen inom nittio (90) dagar från det att de har fått uppgifterna från tjänsteleverantören, om ingen ny ansökan framställs till domstolen.

47. Min erfarenhet och utbildning och den erfarenhet och utbildning som andra utredare som jag har haft kontakt med har, visar att det är nödvändigt att granska och beslagta all e-post som identifierar användare av det ifrågavarande kontot och all e-post som skickas eller tas emot i tidsmässig närhet till misstänkta e-postmeddelanden som kan ge ett sammanhang åt de misstänkta e-postmeddelandena.

48. Vid all kriminalteknisk analys av de kopierade uppgifterna kommer sökprotokoll att användas som uteslutande syftar till att identifiera och extrahera uppgifter inom ramen för denna husrannsakan.

ANSÖKAN OM SEKRETESS OCH YPPANDEFÖRBUD

49. Detta är en pågående utredning som de som utredningen riktar sig mot inte känner till. Denna sofistikerade, hemliga FBI-utredning pågår för närvarande i mer än 90 länder. FBI:s utredning riktar sig mot nästan två dussin av Anomplattformens administratörer och distributörer. Andra länder har påbörjat utredningar mot kriminella användare av dessa enheter. Det ifrågavarande kontot har direkt anknytning till ett mål för FBI:s utredning. Trojan Shield-utredningen beräknas vara avslutad när tredjelandets tillståndsperiod löper ut den 7 juni 2021 och utredningen kommer att offentliggöras den 8 juni. Fram till dess är sekretess kring FBI:s roll i Anom en förutsättning för att utredningen ska fortsätta att ge resultat. Om den som använder och/eller prenumererar på det ifrågavarande kontot skulle delges detta beslut om husrannsakan omgående, skulle det kunna leda till att den som använder det ifrågavarande kontot och hans kumpaner undandrar sig lagföring, förstör bevis (däribland många krypterade enheter) eller på annat sätt allvarligt äventyrar den pågående utredningen genom att påverka den tilltro som de

personer som utredningen riktar sig mot har satt till denna plattform. Dessutom finns det risk för att ett för tidigt röjande kan medföra en fara för informatörens liv och säkerhet. På grundval av det ovan anförda, är det mycket troligt att det finns bevis på de brott som utreds på datorer och enheter som kontrolleras av de personer som utredningen riktar sig mot. Mot bakgrund av detta finns det skäl att anta att ett för tidigt röjande av detta beslut om husrannsakan kan leda till att den bevisningen förstörs eller manipuleras, vilket allvarligt skulle äventyra resultatet av utredningen. Följaktligen yrkas det att detta beslut om husrannsakan och material som har anknytning till det, ska omfattas av sekretess fram till den 7 juni 2021, om domstolen inte beslutar annat.

18. Av samma skäl yrkas det enligt avdelning 18, United States Code, 2705 b §, att domstolen ska ålägga den leverantör av elektroniska datatjänster som denna husrannsakan riktar sig mot, att inte underrätta någon om denna husrannsakan, utöver den personal som är nödvändig för att verkställa husrannsakan, fram till den 7 juni 2021, om domstolen inte beslutar annat.

SLUTSATS

51. Mot bakgrund av det ovan anförda finns det skälig misstanke om att de uppgifter som anges i bilaga B har använts för att begå brott och att de utgör bevis, vinning eller hjälpmedel för brott enligt avdelning 21, United States Code, 841, 846 §§ och att de finns i de lokaler som ska sökas igenom enligt bilaga A.

[Namnteckning]
NICHOLAS I. CHEVIRON
Utredare
Federal Bureau of Investigation

Bevittnat av sökanden i enlighet med kraven i den federala straffprocesslagen P. 4.1 per telefon idag den 17 maj 2021.

[Namnteckning]
MICHAEL S. BERG
FEDERAL DOMARE

Översättning från engelska språket

BILAGA A

Google LLC är en internettjänstleverantör som har sina viktigaste datainformationssystem och andra elektroniska kommunikations- och lagringssystem, register och uppgifter på 1600 Amphitheater Parkway, Mountain View, California 94043.

Översättning från engelska språket

BILAGA B

I. Husrannsakan

Den tjänsteman som genomför husrannsakan ska låta Google LLC, som handhar de datafiler som beskrivs i punkt II nedan, lokalisera filerna och överlämna digitala kopior till tjänstemannen.

II. Uppgifter som ska tillhandahållas av Google LLC

Prenumerant- och/eller användaruppgifter, elektronisk post, bilder, textmeddelanden, telefon- och VoIP-loggar, kontakt- eller vänlistor, profiler, betalningsmetod, detaljerade debiteringsuppgifter, loggåtkomst, backupuppgifter, transaktionsuppgifter och alla andra filer eller uppgifter som har anknytning till följande konto och användarnamn:

expliamdavis@gmail.com

III. Genomsökningen av de uppgifter som Google LLC tillhandahåller enligt detta beslut om husrannsakan ska utföras av FBI i enlighet med ”Rutiner för elektroniskt lagrad information” i den försäkran under ed som har lagts fram till stöd för denna husrannsakan och den kommer att begränsa sig till perioden mellan den 1 januari 2021 och den 17 maj 2021 och till beslag av:

a. Meddelanden, redogörelser och bilagor som syftar till att diskutera eller fastställa skapandet av företag, register, fakturor, transaktioner, uppgifter om konossement, transportuppgifter för att dölja distribution av kontrollerade ämnen eller för att göra testsändningar.

b. Meddelanden, redogörelser och bilagor som syftar till att diskutera den lagliga lasten eller uppgifter om transportmedel som används för att dölja distribution av narkotika eller gör att göra testsändningar.

c. Meddelanden, redogörelser och bilagor som syftar till att identifiera personer eller platser som utgör källan till den dolda narkotikan samt mottagarpersoner och platser och hamnar för den dolda narkotikan.

d. Meddelanden, redogörelser och bilagor som syftar till att identifiera användarna av användarnamnen TOM FORD, Sion och eventuella kumpaner till dem (som Liam Davis) som är inblandade i aktiviteterna i punkt III a–c ovan.

Översättning från engelska språket

e. Meddelanden, redogörelser och bilagor som ger ett sammanhang till de ovan beskrivna meddelandena, exempelvis e-post som skickats eller tagits emot i tidsmässig närhet till relevanta e-postmeddelanden och e-postmeddelanden som syftar till att identifiera användarna av det ifrågavarande kontot.

Vilka utgör bevis på brott enligt avdelning 21, United States Code, 841 a 1 och 846 §§.

Teknisk information om Operation Trojan Shield

Senast uppdaterad: 31 augusti 2021

INNEHÅLLSFÖRTECKNING

1. ÖVERSIKT ÖVER SERVRAR OCH NÄTVERK

För Operation Trojan Shield (OTS) krävdes servrar på flera nivåer för dataöverföring, lagring och granskning.

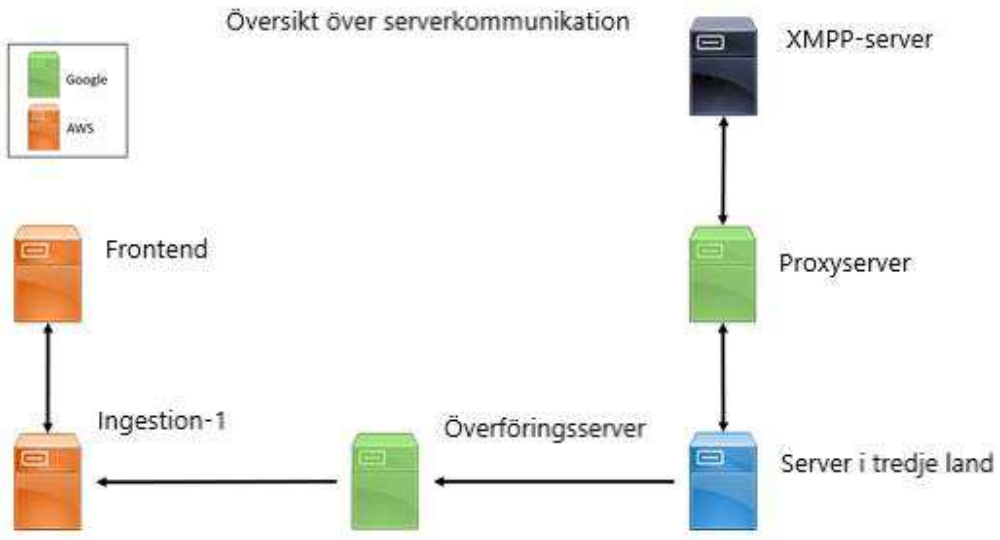


Diagram 1.A

1.1 XMPP-server

XMPP är ett öppet standardprotokoll för snabbmeddelanden som möjliggör chattar mellan flera parter. Det har stöd för multimedia som röst, bilder och video. Vem som helst kan köra en egen XMPP-server och nätverk och bygga vidare på det befintliga ramverket. Appen ANØM innehöll en funktion som innebar att när ett meddelande skickades så skickade appen, via en XMPP-server, automatiskt en dold kopia av meddelandet till ett ghostanvändar-ID, ”bot”. Den här processen var inte synlig för den användare som skickade meddelandet, och den användaren visste inte heller om att processen ägde rum.

1.2 Server i tredje land

En server anskaffades av brottsbekämpande myndigheter i ett tredje land i oktober 2019 för att samla in de dolda kopiorna av meddelanden som skickades till ghostanvändaren ”bot” i enlighet med beskrivning i bilaga A.8 - 59. Servern ägdes, drevs och underhölls av det tredje landet fram tills dess att operationen avslutades.

1.3 Google-servrar

Ett hemligt Google Cloud-konto registrerades för att skapa Google Compute Engines, en tjänst som Google Cloud erbjuder för att skapa och köra virtuella datorer i Google Cloud. De behövdes för att överföra data och tillhandahålla en proxyserver för servern i det tredje landet.

1.3.1 Överföring

Överföringsservern var en konfigurerad Google Compute Engine. Dess enda syfte var att överföra data från servern i det tredje landet till servern Ingestion-1 (I1) i AWS GovCloud.

1.3.2 Proxy

Proxyservern sattes upp som en Google Compute Engine. Servern fungerade som reläserver för alla meddelanden som skickades mellan ANØM-nätverket (XMPP-servern) och uppsamlingsservern i det tredje landet. På så sätt fick man privat kommunikation till ANØM-nätverket från tredjepartsservern.

1.4 AWS GovCloud

Inom AWS GovCloud West konfigurerades, drevs och underhölls EC2-servrar (Elastic Compute Cloud) för OTS.

1.4.1 Säkerhet

AWS-miljön skannas varje månad efter sårbarheter och andra felkonfigurationer som kan utgöra hot. Alla EC2-servrar i AWS GovCloud kör en förstärkt version av operativsystemet CentOS. Båda EC2-servrarna skannas efter sårbarheter och patchas. Skanningen efter sårbarheter och patchningen genomförs enligt de riktlinjer (Security Technical Implementation Guides, STIG) som ges ut av Defense Information Systems Agency (DISA).

1.4.2 Frontend

Frontend-servern fungerade som webbserver för granskningsapplikationen Hola iBot. Mer information om granskningsapplikationen Hola iBot finns i avsnitt 10.

1.4.3 Ingestion-1 (I1)

Ingestion-1 (I1) var den mottagare dit nya datapaket från servern i det tredje landet skickades för behandling och granskning. Den fungerar också som databas och filserver för visning och granskning av data.

1.5 Aktivitet i meddelandenätverket

Som nämns i bilaga A.8 - 59 togs de data som samlades in från plattformen emot som dolda kopior. I diagram 1.B visas en översikt över dataflödet i nätverket för inhämtning av dessa meddelanden.

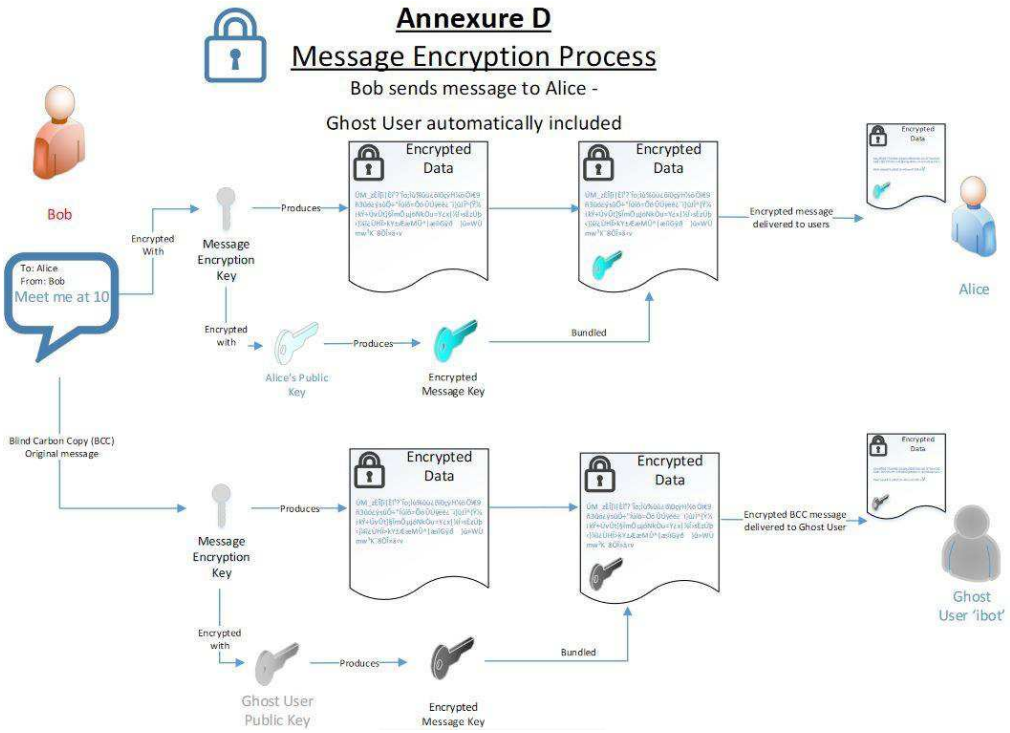


Diagram 1.B

2. SKAPANDE AV NYA DATAPAKET

Tack vare ett avtal om ömsesidig rättshjälp kunde data överföras från det tredje landet varje måndag, onsdag och fredag. En process som gjorde att enbart nya data skickades togs fram och överlämnades till det tredje landet. Följande är en lista över data som bearbetades till nya datapaket:

- MySQL-databasposter:
  - Meddelanden
    - Ett unikt meddelande-ID
      - UUID som unikt identifierar ett enskilt meddelande
    - Avsändare
      - Den avsändande användarens användar-ID (JID)
    - Mottagare
      - Den mottagande enhetens användar-ID (JID) eller grupp-ID (GID)
    - Platsinformation
      - Latitud och longitud bifogades varje meddelande (om enheten tillhandahöll sådan information).
      - Om platsinformation angavs så krypterades den.
    - Mobile Country Code (MCC)
      - Den MCC som meddelandet skickades från
    - Tid
      - Tiden då meddelandet skickades enligt avsnitt 8.6.1
    - Tonhöjdsjustering för ljud
      - Om meddelandet var ett ptt-meddelande (Push To Talk) bifogades ett

värde till bilagan som kunde användas för att ta bort den tonhöjdsjustering som utfördes i appen enligt bilaga A.7.1.4 – 57)

- Typ
  - Varje meddelande kan vara någon av följande typer:
    - text, vidarebefordrat, kontakt
      - Betyder att fältet ”innehåll” innehåller krypterad text
    - ptt, video, bild, anteckning
      - Anger att fältet ”innehåll” innehåller sökvägen till den fil som avsändaren skickade, med filnamnet [unikt meddelande-ID].[bilagans filnamnstillägg]
- Innehåll
  - Om meddelandetypen var ”text”, ”kontakt” eller ”vidarebefordrat” var innehållet krypterat
  - Om meddelandetypen var ”ptt”, ”video”, ”bild” eller ”anteckning” hade fältet sökvägen till den skickade bilagan i klartext

- Förteckning
  - Enhetsanvändar-ID
    - En unik identifierare för en enhetsanvändare
  - Smeknamn
    - Krypterat smeknamn som angavs av användaren
- Gruppinformation
  - Grupp-ID (GID)
    - En unik identifierare för en grupp enheter
  - Gruppnamn
    - Krypterat namn på gruppen som angavs av användaren

- Filer
  - Ljud-, bild-, video- och anteckningsfiler namngavs enligt följande: [Unikt meddelande-ID].[bilagans filnamnstillägg]

2.1 Kryptering av data

Mottagna data (bilagor, innehåll/textmeddelanden, platsinformation, smeknamn och gruppnamn) krypterades med end-to-end-kryptering enligt XMPP-protokollet (Extensible Messaging and Presence Protocol). På servern i det tredje landet avkrypterades data i tillfällig lagring (RAM) vid mottagandet, och sedan krypterades samma data igen med en kombination av asymmetrisk RSA-kryptering och symmetrisk AES-kryptering innan de sparades på disk. Inga data i klartext sparades på servern i det tredje landet. Den privata nyckeln för avkryptering (vad avser RSA) lagrades på I1-servern i AWS GovCloud.

2.2 Hur databasens skillnadsdump skapades

Processen för att erhålla nya data gick ut på att hitta enbart nya data i MySQL-databasen (se ovan för listan över poster som hämtades från databasen). Skillnaden mellan den senaste fullständiga databasdumpen och den nya/aktuella fullständiga databasdumpen kallades internt för ”skillnadsdumpen” (”difference-dump”). Processen inleddes genom att en ny MySQL-databasdump skapades. Databasdumpen från den förra överföringen och den nya databasdumpen användes som indata till ett program. Programmet beräknade skillnaden mellan den förra databasdumpen och den nuvarande och genererade en MySQL-dump med enbart nya data. Se diagram 2.A för en visuell beskrivning av processen.

2.3 Hur listan med bilagor fastställs från skillnadsdumpen

I processen användes skillnadsdumpen för att samla in de nya bilagorna genom att kontrollera fältet ”innehåll” i alla meddelanden som hade sökvägar. Se avsnitt 2 för mer information om var sökvägar lagras som enheter. Som nämndes ovan placerades filnamnen i fältet ”innehåll” om typen inte var ”text”, ”kontakt” eller ”vidarebefordrat’.

2.4 Hur bilagor kopierades från fillagringen

Bilagor lagrades krypterade direkt på servern och programmet som hämtade de nya bilagorna använde sökvägen från fältet ”innehåll” enligt beskrivning i avsnitt 2.3 och kopierade bilagorna till en tillfällig lagringsplats för att skapa paketen.

2.5 Skapa det krypterade paketet

För att paketera MySQL-dumpen med nya data och bilagor komprimerades filerna i en arkivfil med filnamnsillägget ”.tar.gz”. Arkivfilen krypterades med asymmetrisk GnuPG-kryptering (GPG), vilket gjorde att filnamnstillägget ”.gpg” lades till i slutet på arkivets namn. Efter att det krypterade paketet hade skapats hashades det med hashalgoritmen MD5. En hashfunktion är en matematisk process där indata, ”meddelandet”, bearbetas till ett ”sammandrag av meddelandet” eller ett hashvärde med fast längd. Det anges ofta som hexadecimala tecken med siffrorna 0 till 9 och bokstäverna A till F. Hashfunktioner används ofta för dataverifiering genom att identifiera om data har förändrats, eftersom det är mycket osannolikt att två olika ”indatameddelanden” resulterar i samma hashvärde. MD5-hashvärdet sparades till en fil för överföring. I diagram 2.A ges en översikt över paketeringsprocessen.

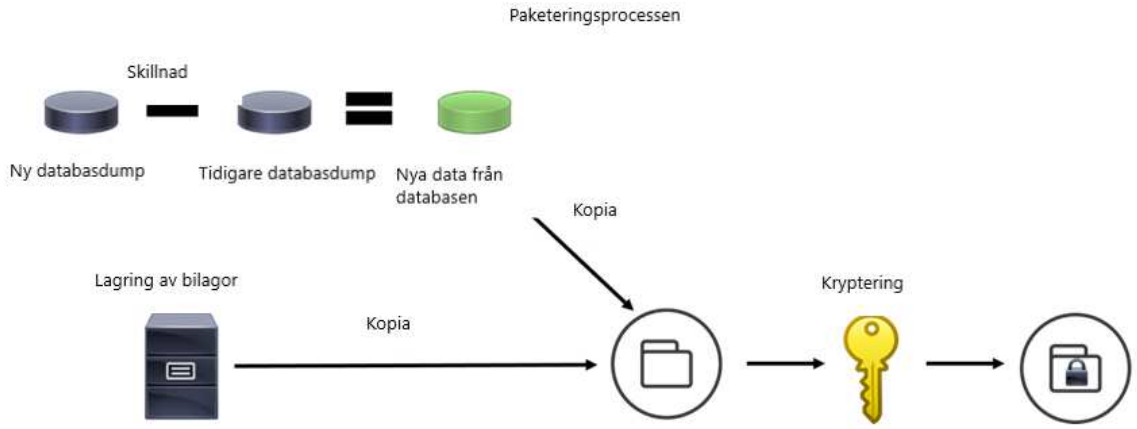


Diagram 2.A

3. ÖVERFÖRING FRÅN SERVERN I DET TREDJE LANDET TILL ÖVERFÖRINGSSERVERN

Det tredje landet körde manuellt ett program som genomförde den behandling av nya data som beskrivs i avsnitt 2.

3.1 Program som överför data till överföringsservern

Varje måndag, onsdag och fredag körde det tredje landet ett program som förpackade och skickade nya data. Programmet skickade MD5-hashvärdet följt av det krypterade paketet med nya data till den hemliga Google Compute Engine-överföringsserver som beskrivs i avsnitt 1.3.1.

4. ÖVERFÖRING FRÅN ÖVERFÖRINGSSERVERN TILL AWS GOVCLOUD

Överföringsservern vidarebefordrade automatiskt mottagna data till I1-servern i AWS GovCloud efter att ha kontrollerat integriteten (genom verifiering av hashvärdet).

4.1 Automatisering av program för att överföra data

När överföringsservern tog emot nya krypterade paket letade den efter filer som slutade med ”.gpg” i den inboxkatalog dit data överfördes. Det indikerade att ett nytt datapaket var klart att överföras till I1 i AWS GovCloud. Programmet beräknade sedan MD5-hashvärdet för .gpg-filen och jämförde det med det MD5-hashvärde som hade överförts av servern i det tredje landet. Om hashvärdena stämde överens betydde det att överföringen hade lyckats och det krypterade paketet vidarebefordrades till I1 i AWS GovCloud.

5. BEARBETNING AV KRYPTERADE PAKET

Varje krypterat paket överfördes till en tilldelad plats på I1 i AWS GovCloud. Genom en automatiserad uppgift kontrollerades om det fanns nya data på platsen. Om nya data hittades på platsen påbörjades inmatningsprocessen på servern.

5.1 Avkryptering av GPG-paket

Först avkrypterades det krypterade paketet med MySQL-data (databasen) samt bilagorna så att dataarkivet (databasen och bilagor till meddelanden) skulle bli tillgängliga. Som nämndes ovan användes asymmetrisk GPG-kryptering för att skydda arkivet med data, så en privat nyckel som enbart var tillgänglig på I1-servern användes för att avkryptera paketet.

5.2 Extrahering av den nya MySQL-databasdumpen och bilagor från arkivet

Efter avkrypteringen extraherades arkivet till filsystemet, vilket gjorde MySQL-datan (databasen) och bilagorna tillgängliga för vidare behandling.

5.3 Inmatning av databasdumpen till en tillfällig databas

I1-servern använde två databaser för behandling av inkommande data. En av dessa databaser, iBot_enc, var en tillfällig lagringsplats för nya data som hade tagits emot från servern i det tredje landet. Här sparades nya MySQL-data tillfälligt för behandling. Nya data behövde avkrypteras, normaliseras och bearbetas in i den andra databasen så att frontend-webbapplikationen Hola iBot kunde visa dessa data.

6. AVKRYPTERINGSPROCESSEN

För att avkryptera och normalisera inkommande data matades databasdumpen in i en databas på I1-servern enligt beskrivningen i avsnitt 5.3.

6.1 Avkryptering av krypterade fält i databasen

Enligt beskrivning i avsnitt 2 krypterades följande fält i databasdumpen:

- Meddelanden
  - Innehåll (om typen är ”text”, ”kontakt” eller ”vidarebefordrat”)
  - Platsinformation (om det finns sådan)
- Förteckning
  - Enhetsanvändarens visningsnamn (se avsnitt 8.3)
    - Kallas också smeknamn, användarnamn, alias
- Gruppinformation
  - Gruppnamn

Med avkrypteringsprocessen avkrypterades fältet ”innehåll” för alla meddelanden utan bilagor direkt

på plats (dvs. det krypterade innehållet ersattes med avkrypterat innehåll) med hjälp av den privata nyckeln för den krypteringsprocess som användes av servern i det tredje landet enligt beskrivning i avsnitt 2.1.

6.1.1 Uppdatering av sökvägar för bilagor så att de är korrekta

När krypterade bilagefiler kom till servern i det tredje landet sparades hela filens sökväg i klartext i fältet ”innehåll” i databasen, om filen var av typen bilaga. Sökvägen avsåg servern i det tredje landet men det här databasfältet användes på samma sätt på I1-servern för att tillhandahålla bilagor för granskning på frontend-webbservern. För att göra bilagorna tillgängliga uppdaterades sökvägen i fältet ”innehåll” till den sökväg där de skulle placeras på I1-servern efter avkryptering och konvertering (om det behövdes).

6.2 Avkryptering av alla filer i bilagor

Efter att sökvägarna i fältet ”innehåll” hade uppdaterats korrekt avkrypterades alla nya filer i bilagor med den privata nyckeln för krypteringsprocessen som användes av servern i det tredje landet enligt beskrivningen i avsnitt 2.1. Genom avkrypteringsprocessen för bilagorna placerades de avkrypterade filerna på rätt plats så att de blev tillgängliga för frontend-webbservern och kunde visas i webbapplikationen Hola iBot.

7. BEARBETNING AV LJUDFILER

Ljudfilerna som kom från servern i det tredje landet behövde bearbetas ytterligare innan de kunde göras tillgängliga i webbapplikationen Hola iBot.

7.1 Konvertera ljudfiler till användbart format

Om en bilaga var en ljudfil (vilket indikerar ett push to talk-meddelande) konverterades ljudfilen, under avkrypteringsprocessen, från filformatet Ogg Opus (OPUS) till filformatet Waveform Audio (WAV). Detta gjordes eftersom webbläsare saknar stöd för OPUS-filer, medan WAV-filer kan spelas upp internt i de flesta moderna webbläsare.

7.2 Ändring av tonhöjd i ljudfiler om nödvändigt

Som nämndes i bilaga A.7.1.4 – 57 fanns det i ANØM-applikationen en möjlighet att justera tonhöjden för det inspelade meddelandet. Användaren hade möjlighet att höja (”helium”) eller sänka (”jellyfish”) tonhöjden i PTT-meddelanden. Tillsammans med varje tonhöjdsjusterat PTT-meddelande skickades också ett värde som representerade den justerade tonhöjden. Värdet användes för att ändra tillbaka tonhöjden, vilket gav en justerad ljudfil. Den tonhöjdsjusterade ljudfilen är tillgänglig för användare av granskningsplattformen Hola iBot, men originalljudfilen sparas också. För närvarande är det dock inte möjligt att återskapa originalljudfilen. Det har inte tagits fram en process för att återskapa originalljudfilen.

8. DATABASÖVERSIKT

Resten av inmatningsprocessen, efter den process som beskrivs i avsnitt 6 och 7, går ut på att omorganisera data i en sekundär databas (iBot_dec). Databasen iBot_dec är den databas som används i frontend-webbapplikationen Hola iBot. I följande avsnitt beskrivs layouten för de viktigaste iBot_dec-tabellerna, liksom interna relationer. Alla tabeller i iBot-dec beskrivs inte i det här avsnittet, men de beskrivs i senare avsnitt om det behövs.

8.1 Ärenden/syndikat

Den centrala komponenten för organisering i databasen iBot_dec är ”ärenden” eller ”syndikat”. I databasen har ärenden ett ärende-ID och ett namn. Ärende-ID är en unik identifierare för ärendet, och namnet är en möjlighet för administratörer att ge ärendet ett namn som är lätt att komma ihåg.

Ärenden har i huvudsak fått namn efter slumpmässigt utvalda gudar och gudinnor i romersk och grekisk mytologi. I databasen finns en tabell med namnet ”ärenden”, där beskrivande information lagras om ärenden.

8.1.1 Grupper av enhetsanvändare (JID)

Ärenden är ett sätt att organisera enhetsanvändare (JID) som ofta pratar med varandra i grupper. De är också ett sätt för användare av granskningsplattformen att skapa en organisationsstruktur.

8.2 Användare av granskningsplattformen

FBI-medarbetare och andra personer från brottsbekämpande myndigheter som övervakar data på plattformen får först ett CJIS LEEP-konto (Law Enforcement Enterprise Portal), men de behöver sedan ytterligare åtkomstbehörigheter för att komma åt granskningsplattformen. För att få dessa behörigheter behöver ett konto skapas i databasen iBot_dec.

Det finns tre huvudsakliga typer av användare i databasen:

- Allmänna användare
- Super users
- Administratörer

I databasen finns en tabell med namnet ”användare”, där beskrivande information lagras om granskningsplattformens användare.

8.2.1 Allmänna användare

Användarna är utredande personal och stödpersonal från FBI och andra brottsbekämpande myndigheter som arbetar med utredningar i Operation Trojan Shield. De har tillgång till produktsidorna för den specifika utredning som de har getts åtkomst till. Produkter i databasen beskrivs närmare i avsnitt 8.5. Här kan de granska, markera och skapa anteckningar om produkter. Allmänna användare kan också komma åt och använda funktionerna i förteckningen. Se avsnitt 8.3 för mer information om förteckningen.

8.2.3 Super users

Super Users är chefer på FBI som ansvarar för utredningar i Operation Trojan Shield. De har tillgång till kommunikationsdata relaterade till deras utredningar på samma sätt som allmänna användare. Super users kan också skapa allmänna användare och ge dem åtkomst till utredningar som de leder.

8.2.4 Administratörer

Administratörer är FBI-personal som är ansvariga för drift, underhåll och övervakning av granskningsplattformen Hola iBot. De granskar behörighetsförfrågningar för att kontrollera att användare har tillräckligt goda skäl för att få åtkomst till Hola iBot och ger användare av granskningsplattformen åtkomst till systemet. Administratörer kan också ge åtkomst till utredningar åt allmänna användare och super users. De har också tillgång till system för att skapa nya ärenden/syndikat.

8.3 Förteckningen

I förteckningen finns all information om enhetsanvändare (JID). Det är en unik lista över alla användare av ANØM-plattformen för vilka data har tagits emot. I databasen finns iBot_dec finns en tabell med namnet ”förteckning”, där beskrivande information lagras om enhetsanvändarna:

- Unik identifierare för enhetsanvändare (JID)
    - Varje användare i ANØM identifieras med en unik identifierare (användar-ID), som tekniskt kallas för en Jabber Identifier (JID). Från början hade användar-ID formen av 6 alfanumeriska tecken (till exempel ”aab2c3”) som genererades automatiskt från

enhetens IMEI-nummer (International Mobile Equipment Identity number) (bilaga A.3 – 19 och A.7.1.1 – 46).

- Enhetsanvändarens visningsnamn
  - Användaren av enheten kunde ange ett ”visningsnamn” (som också kallas smeknamn, användarnamn eller alias), som kunde ändras när användaren ville. Det förändrade inte deras användar-ID (JID) på plattformen (bilaga A.7.1.2 – 47)
- Verkligt namn
  - Om en enhetsanvändares verkliga identitet kunde fastställas genom granskning av innehållet finns det ett utrymme där den kan anges.
- Biografi
  - I granskningsplattformen går det att ange ytterligare information som har samlats in om en enhetsanvändare som kan vara bra att ha med i deras JID-profil. JID-profilen diskuteras närmare i avsnitt 10.7.
- Plats
  - Om man under granskning av en enhetsanvändares eller andra användares innehåll upptäcker en förmodad plats för en enhetsanvändare går det att ange den informationen i granskningsplattformen.

8.4 Grupper

Enligt beskrivningen i bilaga A.7.1.4 – 51 kunde en enhetsanvändare också skicka end-to-end-krypterade meddelanden till en grupp av ANØM-användare, och varje användare i den gruppen kunde se de andra medlemmarna i gruppen. Grupper fick också namn som enhetsanvändarna kunde definiera. Mer information om grupper finns i bilagan, avsnitt A.7.1.4 – 51.

Databasen iBot_dec hade en tabell med namnet ”grupper”, som rymmer följande information:

- Grupp-ID (GID)
  - GID är en sträng alfanumeriska tecken som unikt identifierar en grupp.
  - GID:n tilldelas på samma sätt som JID:n, på XMPP-servern.
- Namn
  - Det användardefinierade namnet på en grupp.
- Infogad
  - Datumet för det nya datapaket som först innehöll information om gruppen. Mer

information om hur enhetsanvändare är kopplade till grupper finns i avsnitt 8.7.4.

8.4.1 Avsaknad av gruppinformation

Gruppinformation samlades inte alltid in under den period då datapaket togs emot från det tredje landet. Informationen om grupper i databasen är därför inte fullständig.

8.5 Produkter

Produkter är synonymt med konversationer som finns i varje nytt datapaket. En produkt representerar en konversation mellan två eller flera enhetsanvändare i ett ärende under tidsperioden mellan det föregående datapaketet och datapaketet med den nuvarande produkten.

8.5.1 Produkter i detalj

En ny unik uppsättning produkter skapas med varje nytt datapaket som tas emot från det tredje landet för varje ärende. Mer information om hur produkter skapas finns i avsnitt 9.

I databasen iBot_dec finns en tabell som heter ”produkter”. I den tabellen finns följande information:

- Ärende-ID
  - Varje produkt som skapas har en en-till-en-relation med ett ärende.
  - Den unika identifieraren för det ärende/syndikat som produkten tillhör lagras i produkttabellen i form av ett positivt heltal.
- Produkt-ID (PID)
  - En unik identifierare för produkten i form av ett positivt heltal.
- Produktanteckning
  - Användare av granskningsplattformen kan lägga till anteckningar i produkter.
  - Anteckningarna läggs till i det här fältet.
- Skapad datum
  - Nya datapaket tas emot från det tredje landet varje måndag, onsdag och fredag.
  - Eftersom nya uppsättningar produkter skapas varje gång ett nytt datapaket tas emot sparas också datumet då produkten genererades, vilket är detsamma som datumet då det nya datapaketet skapades.
- MCC-sträng
  - En unik lista över de olika MCC-koder (Mobile Country Codes) som används av enheterna i produkten.
- JID-sträng
  - En lista i alfabetsordning med unika identifierare för enhetsanvändare (JID) som skickade eller tog emot meddelanden i produkten.
- Antal meddelanden
  - Antalet meddelanden i produkten.
- JID 1
  - Den första avsändaren av ett meddelande i produkten.
- JID 2
  - Den andra deltagaren eller JID i produkten om produkten inte är en grupprodukt.
- Grupp-ID (GID)
  - Gruppens unika identifierare om produkten är en grupprodukt
- Är dubblett
  - Det här värdet är antingen 1 eller 0 (1 = dubblett, 0 = inte dubblett).
  - Som nämnts ovan har varje produkt en en-till-en-relation med ett ärende.
    - Om en eller flera JID i en produkt inte alla tillhör samma ärende eller syndikat (t.ex. JID 123456 tillhör ärende Alfa och JID 789100 tillhör ärende Bravo) skapas en produkt för varje ärende.
    - Produktens meddelanden och deltagare kommer att vara samma, men det kommer att skapas en produkt för varje ärende som en JID i produkten hör till.
    - Se avsnitt 8.7.3 för mer information om relationer mellan JID och ärenden i databasen och avsnitt 9 för mer information om inmatningsprocessen.
- Känd grupp
  - Det här värdet är antingen 1 eller 0 (1 = databasen har information om gruppen, 0 = databasen har inte information om gruppen).
  - Som nämndes ovan i avsnitt 8.4.1 samlades gruppinformation inte alltid in på servern i

det tredje landet.

- Om gruppinformation saknas kan inte granskningsplattformen Hola iBot visa gruppens identifierare och gruppnamnet, och eventuellt inte **alla** gruppmedlemmar.
- Men produkterna bildas direkt från meddelandena och medlemmarna i konversationen/gruppen fastställs av avsändare och mottagare av meddelanden.
- Även om databasen inte innehåller gruppinformation kommer JID-strängen alltså ändå att spegla medlemmarna i konversationen/produkten.

8.6 Meddelanden

MySQL-skillnadsdumpen i det nya datapaketet som togs emot från det tredje landet innehöll en enda tabell för meddelanden. Mer detaljerad information om inmatningsprocessen för meddelanden finns i avsnitt 9. Det finns fyra tabeller i databasen iBot_dec med meddelandeinnhåll och associerade metadata:

- ”textmeddelande”
  - I den här tabellen finns avkrypterade textmeddelanden, kontaktmeddelanden, vidarebefordrade meddelanden och textkomponenter i anteckningsmeddelanden.
  - I tabellen finns även fältet ”från anteckning”, vilket anger att texten i fältet ”innehåll” kommer från ett meddelande av typen anteckning.
    - Se avsnitt 9.3.2.2.2 för mer information om hur meddelanden av typen anteckning matas in i databasen.
- ”ptt-meddelande”
  - I den här tabellen finns sökvägar (på I1-servern) för avkrypterade, konverterade och tonhöjdsjusterade (vid behov) push-to-talk-meddelanden.
- ”videomeddelande”
  - I den här tabellen finns sökvägar (på I1-servern) för avkrypterade videomeddelanden.
- ”bildmeddelande”
  - I den här tabellen finns sökvägar (på I1-servern) för avkrypterade bildmeddelanden och bildkomponenter i anteckningsmeddelanden.
  - I tabellen finns även fältet ”från anteckning”, vilket anger att bilden som finns i sökvägen i fältet ”innehåll” kommer från ett meddelande av typen anteckning.
    - Se avsnitt 9.3.2.2.2 för mer information om hur meddelanden av typen anteckning matas in i databasen.

I alla fyra tabeller finns följande metadatafält:

- Meddelande-ID (MID)
  - En unik identifierare för ett meddelande i form av ett positivt heltal.
  - MID delas av alla fyra tabellerna.
    - Om t.ex. MID 5 visas i ptt-meddelande så visas inte samma MID någon annanstans.
- Ursprungligt meddelande-ID
  - En annan unik identifierare för ett meddelande som kommer från de nya datapaketen.
  - En unik sträng av tecken som representeras som ett UUID (Universally Unique Identifier).
  - Detta meddelande-ID sparades med varje meddelande som servern i det tredje landet tog emot som en dold kopia.
  - Detta meddelande-ID beskrivs närmare i bilaga A.8.2 – 64.a.

    - MID skapades i databasen iBot_dec för att skapa en enhetlig standard för primära nycklar i databasen.
        - T.ex. PID:n som positiva heltal, ärende-ID:n som positiva heltal osv.
- Datum för infogande
    - Datum för infogande är det datum då datapaketet som innehöll meddelandet matades in i databasen.
- MCC (Mobile Country Code)
    - MCC för den avsändande enheten vid tidpunkten då meddelandet skickades.
- Är grupp
    - Det här värdet är antingen 1 eller 0 (1 = meddelandet skickades till en grupp, 0 = meddelandet skickades inte till en grupp).
    - Om meddelandet är ett gruppmeddelande (värdet 1) innehåller fältet mottagare det grupp-ID (GID) som meddelandet skickades till.
- Avsändare
    - Den avsändande enhetens användar-ID (JID)
- Tid
    - Tiden då meddelandet skickades enligt avsnitt 8.6.1.
    - Ett meddelande som skickades den 6 juni 2021 kl. 22.00 Pacific Time skulle i databasen ha tiden och datumet angivet som kl. 05.00 den 7 juni 2021 UTC.
- Platsinformation
    - Om platsinformation (latitud och longitud) mottogs med ett meddelande lagrades latitud och longitud med varje meddelande i var och en av de fyra tabellerna.

8.6.1 Fel i meddelandens tidszon

På grund av en felkonfiguration på servern i det tredje landet varierade meddelandenas tidszoner under inhämtningsperioden. Följande tidsramar visar den korrekta konverteringen av tidsstämplar för meddelanden:

- Tidsram 1
    - 1 oktober 2019 – 27 oktober 2019: UTC – 3
- Tidsram 2
    - 27 oktober 2019 – 29 mars 2020: UTC – 2
- Tidsram 3
    - 29 mars 2020 – 18 september 2020: UTC – 3
- Tidsram 4
    - 18 september 2020 – operationens slut: UTC

8.7 Relationer

I följande avsnitt definieras de relationer i iBot_dec som motsvarar alla de tabeller som definieras i avsnitt 8.1-8.6. Alla de tabeller som definieras i avsnitt 8.7 har många-till-många-relationer, och de följer denna namngivningskonvention:

Användare **tilldelad_till** *ärende*

Där text i kursiv stil är tabeller med en nyckel (den unika posten i tabellen användare identifieras unikt av användar-ID) och texten i fet stil anger att tabellen har sammansatta nycklar (den unika posten i tabellen tilldelad_till identifieras unikt med både ett användar-ID och ett ärende-ID).

8.7.1 Relation produkt till meddelande

I databasen iBot_dec finns en tabell som heter ”har_meddelande”. I den tabellen finns följande information:

- Produkt-ID (PID)
  - En unik identifierare för produkten i form av ett positivt heltal som meddelandet i samma rad med värden är relaterad till.
- Meddelande-ID (MID)
  - En unik identifierare för meddelandet i form av ett positivt heltal som produkten i samma rad med värden är relaterad till.
- Typ
  - Den meddelandetyp som hänvisas till med meddelande-ID i samma rad med värden.
- Markering
  - Varje meddelande kan ha markeringen ”inte markerad”, ”relevant”, ”inte relevant” eller ”privat”.
- Ursprungligt meddelande-ID
  - Den unika teckensträng i form av ett UUID (Universally Unique Identifier) som unikt identifierar ett meddelande. Härrör från det ursprungliga datapaket som meddelandet hörde till.

8.7.2 Relation mellan användare och åtkomst till ärenden

Användare av granskningsplattformen får explicit åtkomst till ärenden av administratörer. Relationen mellan användare av granskningsplattformen och ärenden hanteras genom tabellen ”tilldelad_till”. Tabellen ”tilldelad_till” innehåller följande attribut:

- LEEP-användarnamn
  - Användarnamnet för den Hola iBot-användare som har åtkomst till det ärende som identifieras i samma rad med värden.
- Ärende-ID
  - Ärende-ID för det ärende som Hola iBot-användaren i samma rad med värden har åtkomst till.

8.7.3 Relationen mellan JID och ärenden

Enhetsanvändare (JID:n) tilldelas till ärenden som ett sätt att gruppera dem med andra enhetsanvändare som ofta kommunicerar med varandra, enligt beskrivning i 8.1.1. Eftersom många enhetsanvändare kan motsvara många ärenden är sådana relationer möjliga i tabellen ”tillhör”. Tabellen ”tillhör” innehåller följande attribut:

- Enhetsanvändar-ID
  - JID för den användare som är relaterad till ärende-ID:t i samma rad med värden
- Ärende-ID
  - Det ärende-ID som motsvarande JID är relaterat till.
- Datum för skapande
  - Det datum då relationen skapades i databasen iBot_dec.

8.7.4 Relationen mellan JID och grupper

Enhetsanvändare (JID:n) läggs till i grupper av gruppadministratörer i applikationen ANØM. JID:n kan vara medlemmar i många grupper, och grupper kan ha många JID:n som är medlemmar. Denna relation är alltså tillåten i tabellen ”medlem_i”. Tabellen ”medlem_i” innehåller följande attribut:

- Enhetsanvändar-ID
  - JID för den användare som är medlem i den grupp som identifieras i samma rad med värden
- Grupp-ID (GID)
  - GID för den grupp som motsvarande JID är medlem i.

9. INMATNINGSPROCESS

Efter avkrypteringen av alla krypterade innehållsfält, smeknamn i förteckningen, gruppnamn och bilagor, liksom justering av sökvägar i fältet ”innehåll” för meddelanden av typen ptt, video, bild eller anteckning fortsätter inmatningsprocessen med de steg som beskrivs i det här avsnittet (avsnitt 9). I det här avsnittet beskrivs processen för att överföra data på I1 från databasen iBot_enc (där nya datapaket sparades tillfälligt) till databasen iBot_dec, som ger granskningsplattformen tillgång till nya data.

Förutsättningarna för att inleda inmatningsprocessen anges i avsnitt 5-7:

- Avkryptera det krypterade nya datapaketet
- Extrahera dataarkivet
  - Filer i bilagor
  - MySQL-skillnadsdumpen
    - Enligt beskrivningen i avsnitt 2.2 innehåller skillnadsdumpen bara nya eller annorlunda data.
- Mata in MySQL-skillnadsdumpen i den tillfälliga databasen iBot_enc
- Avkryptera alla krypterade fält i databasen
- Korrigera sökvägar i alla fält i databasen som hänvisar till filer i bilagor
- Avkryptera alla filer i bilagor
- Konvertera och tonhöjdsjustera ljudet, om det behövs

9.1 Mata in ny information i förteckningen

De första dataposterna som infogas i databasen iBot_dec är förteckningsinformationen. Följande process används för att lägga till ny information i förteckningen:

1. Läs in alla nya förteckningsdata från iBot_enc (nya MySQL-data)
2. För varje ny post i förteckningen:
   a. Kontrollera om enhetsanvändar-ID:t (JID) redan finns i tabellen ”förteckning” i iBot_dec
   b. Om enhetsanvändaren redan finns indikerar det att användaren har ändrat sitt visningsnamn för enhetsanvändare.
      i. Om det nya visningsnamnet inte stämmer överens med det gamla visningsnamnet uppdateras det nya visningsnamnet i tabellen ”förteckning” i iBot_dec.
   c. Om enhetsanvändaren inte existerar indikerar det att det är en helt ny användare. Användaren läggs till i tabellen ”förteckning” i iBot_dec och en relation läggs till för enhetsanvändaren så att den motsvarar ärendet ”OKÄND”.
      i. Ärendet ”OKÄND” är ett standardärende där alla nya enhetsanvändare (JID) och enheter placeras tills dess att man hittar ett ärende eller ett syndikat där de kan placeras.

Eventuella fel som uppstår när enhetsanvändares visningsnamn uppdateras eller när användaren infogas i tabellen ”förteckning” loggas.

9.2 Infoga nya grupper

9.2.1 Infoga ny gruppinformation

Ny information om grupper i ANØM-plattformen matas in efter den nya förteckningsinformationen. Följande process används för att lägga till ny gruppinformation:

1. Läs in alla nya gruppdata från iBot_enc (nya MySQL-data)
2. För varje grupp i nya data:
    a. Grupp-ID (GID), gruppnamn och datum för infogande matas in i tabellen ”grupper” i databasen iBot_dec.

9.2.2 Infoga uppdateringar om medlemskap i grupper

Medlemmar lades till i grupper på ANØM-plattformen av gruppadministratörer, och dessa uppdateringar togs emot i MySQL-skillnadsdumpen. Följande process används för att uppdatera relationen gruppmedlemskap:

1. Läs in alla nya data om gruppmedlemskap från iBot_enc (nya MySQL-data)
2. För varje ny relation mellan grupp-ID (GID) och enhetsanvändar-ID (JID):
    a. GID och JID matas in i tabellen ”medlem_i” i databasen iBot_dec.

9.3 Inmatning av meddelanden

Efter att förändringar i förteckningen och grupper har uppdaterats i databasen inleds processen för att mata in meddelanden. Det här är den primära inmatningsmekanismen som gör det möjligt att granska data i form av produkter (konversationer). Inmatning av meddelanden följer den process som beskrivs i det här avsnittet (9.3).

9.3.1 Initialisering

Innan nya data matas in initialiseras vissa komponenter.

9.3.1.1 Svart lista

Den svarta listan är en radavgränsad textfil som separerar JID:n. I filen finns JID:n vars skickade meddelanden är svartlistade från att matas in i databasen iBot_dec. Svartlistningsfunktionen kommer att beskrivas närmare i ett framtida tillägg.

9.3.1.2 Tillfällig datastruktur för konversationer

Datastrukturen som ska innehålla alla unika konversationer och de meddelanden som motsvarar dem initialiseras. Det här är de data som används för att skapa produkter efter att alla nya meddelanden har gåtts igenom.

9.3.1.3 Tillfällig datastruktur för ärende-till-JID

Det här är en datastruktur med en lista över JID:n som hör till varje ärende i databasen. Datastrukturen kommer att användas senare för att skapa korrekta produkter. Den skapas från data i tabellen ”tillhör”.

9.3.1.4 Hämta senaste meddelande-ID (MID)

Genom att hämta det senast infogade meddelande-ID:t (MID) får man fram det meddelande-ID (MID) som är först i de nya data, eftersom MID är stigande positiva heltal.

9.3.1.5 Läs in nya meddelanden

De nya meddelandena läses in från iBot_enc (nya MySQL-data) för att infogas.

9.3.2 Infoga meddelanden

För varje meddelande genomförs sedan resten av åtgärderna i avsnitt 9.3.2.

9.3.2.1 Infoga metadata

I databasen iBot_dec finns en tabell med namnet ”metadata” som innehåller de data som har gemensamma attribut från alla de fyra meddelandetabeller som beskrivs i avsnitt 8.6. Tabellen ”metadata” innehåller följande attribut:

- Meddelande-ID (MID)
- Ursprungligt meddelande-ID
- Tid
- Avsändare
- Mottagare
- Mobile Country Code (MCC)
- Är grupp
- Typ
- Platsinformation

Alla attributen ovan definieras i avsnitt 8.6 i avsnittet om metadata. Alla metadataattribut infogas för alla meddelanden oavsett meddelandetyp.

9.3.2.2 Infoga efter typ

Inmatningsprocessen skiljer sig åt beroende på meddelandetyp.

9.3.2.2.1 Meddelanden av typerna ”text”, ”kontakt” och ”vidarebefordrat”

Om meddelandetypen är ”text”, ”kontakt” eller ”vidarebefordrat” kopieras fältet ”innehåll” från meddelandetabellen i iBot_enc till fältet ”innehåll” i tabellen ”textmeddelande” i iBot_dec. Värdet i fältet ”innehåll” avkrypterades genom stegen i avsnitt 6.1.

9.3.2.2.2 Meddelanden av typen ”anteckning”

Om meddelandetypen var ”anteckning” avkrypterades anteckningsbilagan. Efter avkrypteringen visas anteckningsbilagor som komprimerade ZIP-filer som innehåller text- och bildfiler. Filerna fördelas ut i tabellerna ”textmeddelande” och ”bildmeddelande”.

Först extraheras ZIP-filerna för bearbetning. För varje extraherad fil fastställs först huruvida filen är en textfil eller en bildfil. Om det är en textfil läses texten och infogas i fältet ”innehåll” i tabellen ”textmeddelande”. Om det däremot är en bildfil kopieras bildfilen till den katalog som användes för att skicka bilder till frontend-webbapplikationen, och en datapost infogas i tabellen ”bildmeddelande”.

Alla poster som infogades i ”textmeddelande” eller ”bildmeddelande” fick attributet ”från anteckning” uppdaterat till värdet 1 för att visa att texten/bilden är en komponent från en anteckning.

9.3.2.2.3 Meddelanden av typerna ”ptt”, ”bild” och”video”

Om meddelandetypen är ”ptt”, ”bild” eller ”video” kopieras fältet ”innehåll” direkt från meddelandetabellen i iBot_enc till motsvarande meddelandetabell (beroende på typ) i iBot_dec. Sökvägarna i fältet ”innehåll” korrigerades på plats och uppdaterades till de nya sökvägar som användes av frontend-webbapplikationen för granskning. Mer information om hur sökvägarna uppdateras finns i avsnitt 6.1.1.

9.3.4 Tilldela meddelanden till produkter

Efter att tabellen metadata har fyllts på och infogandet i tabeller efter typ har slutförts placeras meddelandet i en konversation med hjälp av den tillfälliga datastruktur som initialiserades i avsnitt 9.3.1.2.

Den här datastrukturen innehåller en kapslad unik lista med konversationer som alla innehåller deltagarna (JID) i konversationen, MCC-koder (Mobile Country Codes) som meddelandena skickades från, meddelande-ID (MID) och meddelandetypen (”text”, ”ptt”, ”video” osv.).

Efter att alla meddelanden har placerats i en konversation är processen för nya meddelanden klar och användandet av den tillfälliga databasen iBot_enc avslutas.

9.4 Inmatning av produkter

När konversationsdata har fyllts i är produkterna redo att skapas för det nya datapaketet. I resten av avsnitt 9.4 bearbetas varje unik konversation i den tillfälliga datastruktur som innehöll meddelanden.

9.4.1 Skapa produkter per ärende

För varje ärende verkställs stegen under 9.4.1.1 för konversationen.

9.4.1.1 Om JID i konversationen tillhör ett ärende

Om en enhetsanvändare som är deltagare i den aktuella konversationen tillhör det aktuella ärendet gås stegen 9.4.1.1.1- 9.4.1.1.3 igenom.

9.4.1.1.1 Skapa produkt för ärenden

Om 9.4.1 och 9.4.1.1 har genomgåtts för den aktuella konversationen skapas en produkt för det aktuella ärendet. Följande värden infogas baserat på tillfälliga datastrukturer och nuvarande status för inmatningskoden:

- Ärende-ID
- Skapad datum
- MCC-sträng (Mobile Country Code)
- Enhetsanvändar-ID-sträng (JID)
- Antal
- Grupp-ID (GID) – om det behövs
- Känd grupp – Om gruppinformation hittades under skapandet av produkten (genom sökning i tabellen ”grupper”) sätts det här värdet till 1.

9.4.1.1.2 Skapa relation för meddelande och JID till produkt

Som nämndes i avsnitt 8.7.1 är meddelanden associerade med produkter genom användning av tabellen ”har_meddelande”. Efter att produkten har skapats för det aktuella ärendet associeras alla meddelanden i den tillfälliga konversationsdatastrukturen med produkten genom att deras meddelande-ID:n (MID) infogas i ”har_meddelande” tillsammans med det produkt-ID (PID) som infogades.

Det finns en tabell i databasen iBot_dec som heter ”del_av” som kopplar enhetsanvändar-ID:n (JID) till produkt-ID:n (PID). Då skapas en tabell som informerar systemet om att en specifik användare har skickat meddelanden som syns i en produkt. Den tabellen innehåller följande attribut:

- Enhetsanvändar-ID
- Produkt-ID (PID)

Tabellen fylls också i när en ny produkt skapas.

9.4.1.1.3 Tilldela standardmarkering till produkt

Det finns en tabell i databasen iBot_dec med namnet ”har_markering” där textbaserade

markeringar kopplas till produkter. Produkter kan markeras i granskningsplattformen Hola iBot av Hola iBot-användare. Tabellen ”har_markering” innehåller följande attribut:

- Produkt-ID (PID)
- Markering
    - En textbaserad markering som kan sättas på en produkt.
    - Markeringen kan t.ex. vara inte granskad (standardmarkering), relevant eller inte relevant.

Standardproduktmarkeringen inte granskad infogas i tabellen ”har_markering” för den produkt som genereras.

9.5 Export efter inmatning

Krypterade exporter skickades automatiskt via SFTP (Secure File Transfer Protocol) till länder som omedelbart behövde granska nya data i datapaket. Dessa krypterade exporter innehöll en JSON-fil (JavaScript Object Notation) för varje ärende som landet ifråga hade getts åtkomst till. JSON-filen innehöll alla produktdata för det tidigare inmatade datapaketet.

10. WEBBAPPLIKATION/GRANSKNINGSPLATTFORM

Hola iBot är den anpassade webbapplikation som har skapats och drivs av FBI i San Diego och som fungerar som granskningsplattform för alla data som har tagits emot från ANØM-plattformen.

10.1 Kontroll av användaråtkomst i Hola iBot

De användarroller för granskningsplattformen som definieras i avsnitt 8.2 är roller för användare av Hola iBot. Som har nämnts tidigare måste alla användare i avsnitt 8.2 först få konton i LEEP (Law Enforcement Enterprise Portal).

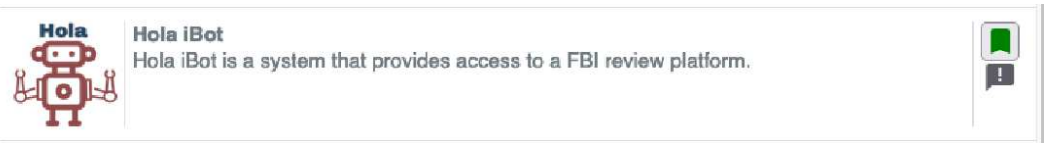
10.1.1 Åtkomstkontroll för LEEP (Law Enforcement Enterprise Portal)

LEEP (Law Enforcement Enterprise Portal) är en portal som brottsbekämpande myndigheter (även internationella sådana) och andra underrättelsegrupper kan få konton i. När avdelningen som ger åtkomst har granskat den ansökande användaren ges användaren åtkomst till listan med applikationer/verktyg. Ett av dessa är granskningsportalen Hola iBot.

LEEP använder gemensamma metoder för autentisering av användare, t.ex. tvåfaktorautentisering (2FA), säkerhetsbilder och säkerhetsfrågor.

10.1.2 Åtkomstkontroll i Hola iBot

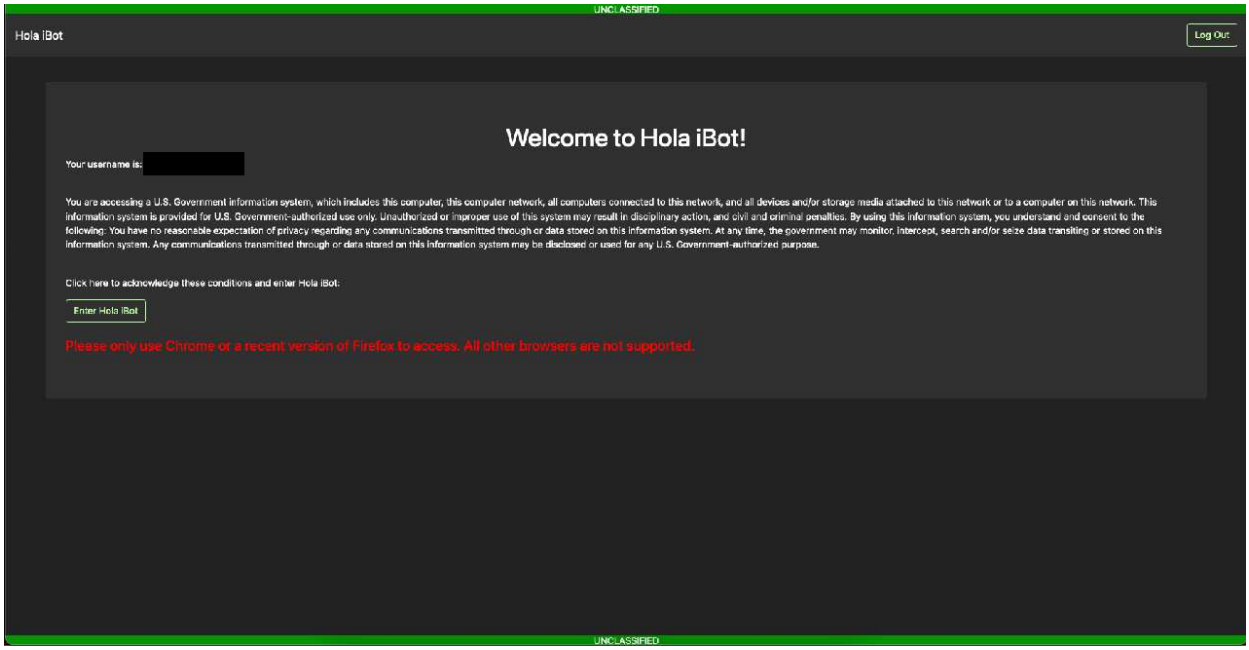
När en användare har autentiserat sig genom den LEEP-administrerade inloggningsprocessen kan användaren öppna applikationen Hola iBot genom att klicka på applikationen i listan som visas i skärmbilden nedan.



Skärmbild 10.A

När man klickar på applikationen Hola iBot skickas en SSO-begäran (single sign-on) i SAML (Security Assertion Markup Language) till frontend-servern för webbapplikationen. SAML är ett protokoll som gör det möjligt för identitetsleverantörer att skicka autentiserade inloggningsuppgifter till en annan tjänst, och det är så Hola iBot autentiserar användare.

Användaren av granskningsplattformen ges bara åtkomst till systemet om de finns upptagna i tabellen ”användare” som omnämns i avsnitt 8.2. Om de ges behörighet till applikationen hälsas de av varningsmeddelandet i skärmbild 10.B.

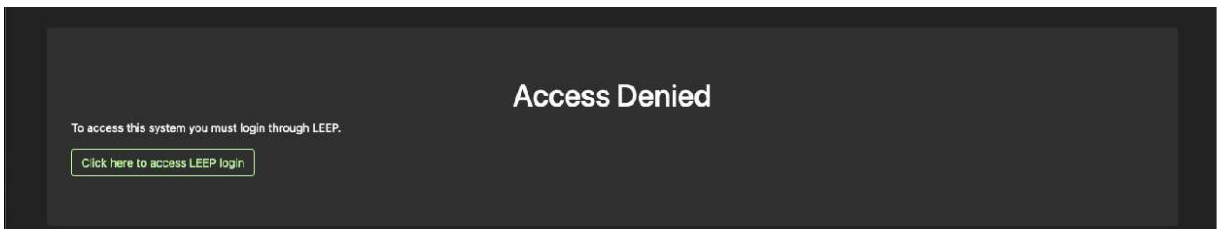


Skärmbild 10.B

Texten i varningsmeddelandet är följande (översatt till svenska):

> *Du ansluter till ett informationssystem som ägs av USA:s federala regering. Det omfattar den här datorn, det här datornätverket, alla datorer som är anslutna till det här nätverket och alla enheter och/eller lagringsmedia som är anslutna till det här nätverket eller till en dator i det här nätverket. Informationssystemet tillhandahålls enbart för användning som är godkänd av USA:s federala regering. Obehörig eller oriktig användning av systemet kan leda till disciplinära åtgärder samt civil- och straffrättsliga sanktioner. Genom att använda det här informationssystemet förstår du och ger ditt samtycke till följande: Du kan inte förvänta dig någon form av personlig sekretess gällande någon form av kommunikation som genomförs på det här systemet, eller gällande data som lagras på det. USA:s federala regering kan när som helst övervaka, avläsa, genomsöka och/eller beslagta data som passerar igenom eller lagras på det här informationssystemet. All kommunikation som skickas, och alla data som lagras, på det här informationssystemet kan röjas eller användas för vilket syfte som helst som är godkänt av USA:s federala regering.*

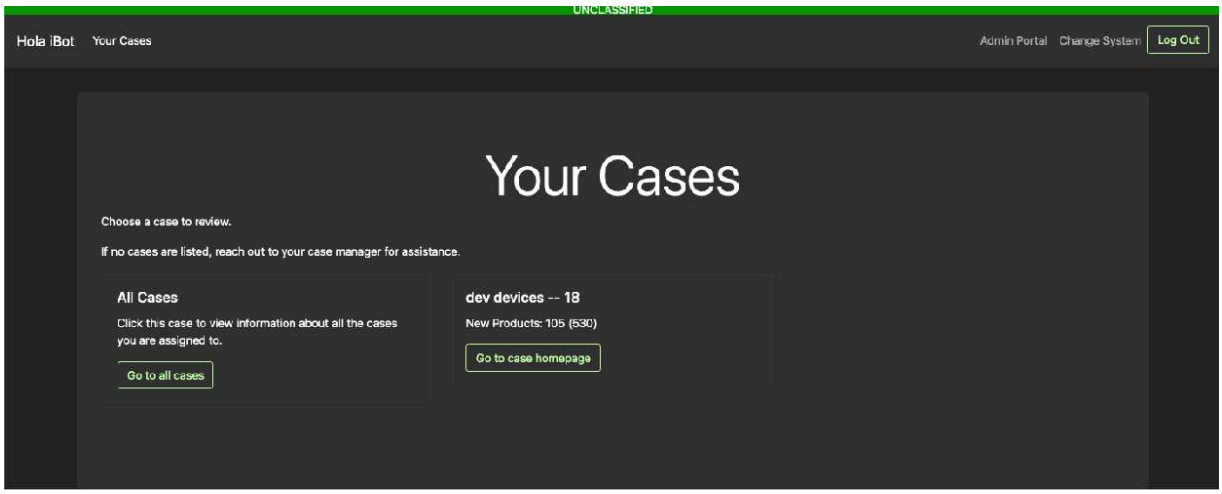
Om användaren inte finns i databasen ser de en generisk sida om nekad åtkomst. Den sidan visas i skärmbild 10.C.



Skärmbild 10.C

10.2 Ärenden i Hola iBot

Om användaren får åtkomst till systemet genom LEEP-autentisering och explicit åtkomst till databasen Hola iBot kommer användaren till sin hemsida, där det visas en lista med ärenden som användaren har fått explicit åtkomst till. I skärmbild 10.D visas hemsidan för en användare som har åtkomst till ett enda ärende, ”dev devices”, med ärende-ID 18.



Skärmbild 10.D

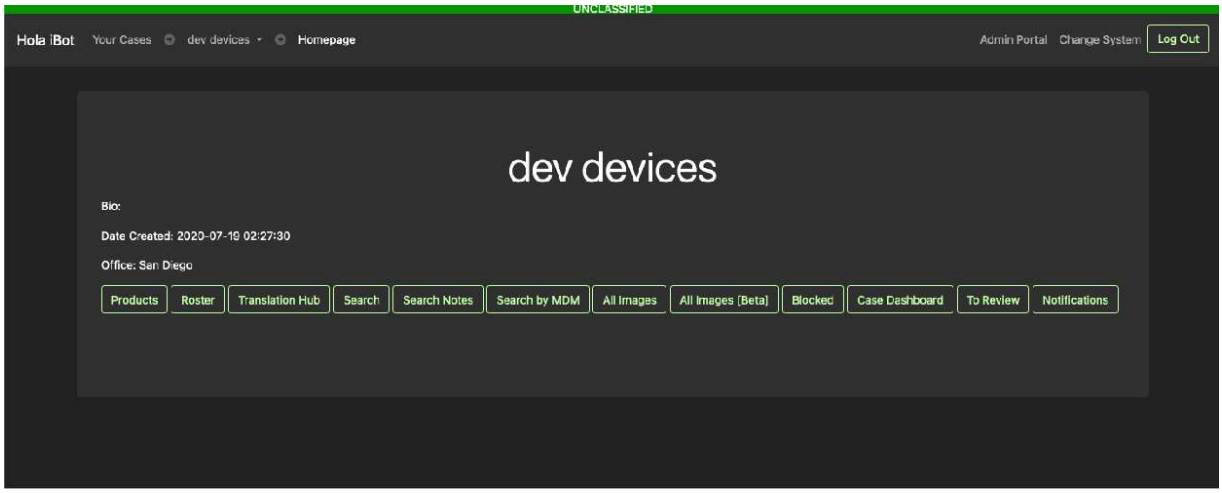
Listan med ärenden som visas på hemsidan baseras på tabellen ”tilldelad_till” enligt beskrivningen i avsnitt 8.7.2 ovan.

Vid visning av ett enda ärende filtreras data på de återstående sidorna till enbart de enhetsanvändare (JID) som är kopplade till ärendet i tabellen ”tillhör” (relationen mellan JID och ärende-ID), enligt beskrivningen i avsnitt 8.7.3.

Användarna har också alternativet ”alla ärenden”. Om det alternativet väljs blir de återstående sidorna ifyllda med alla data som användaren av granskningsplattformen har åtkomst till.

10.2.1 Ärendets hemsida

När en användare av granskningsplattformen har navigerat till ett ärende visas hemsidan för det ärendet. På ett ärendes hemsida visas flera alternativ. Ett exempel på en hemsida för ett ärende visas i skärmbild 10.E.



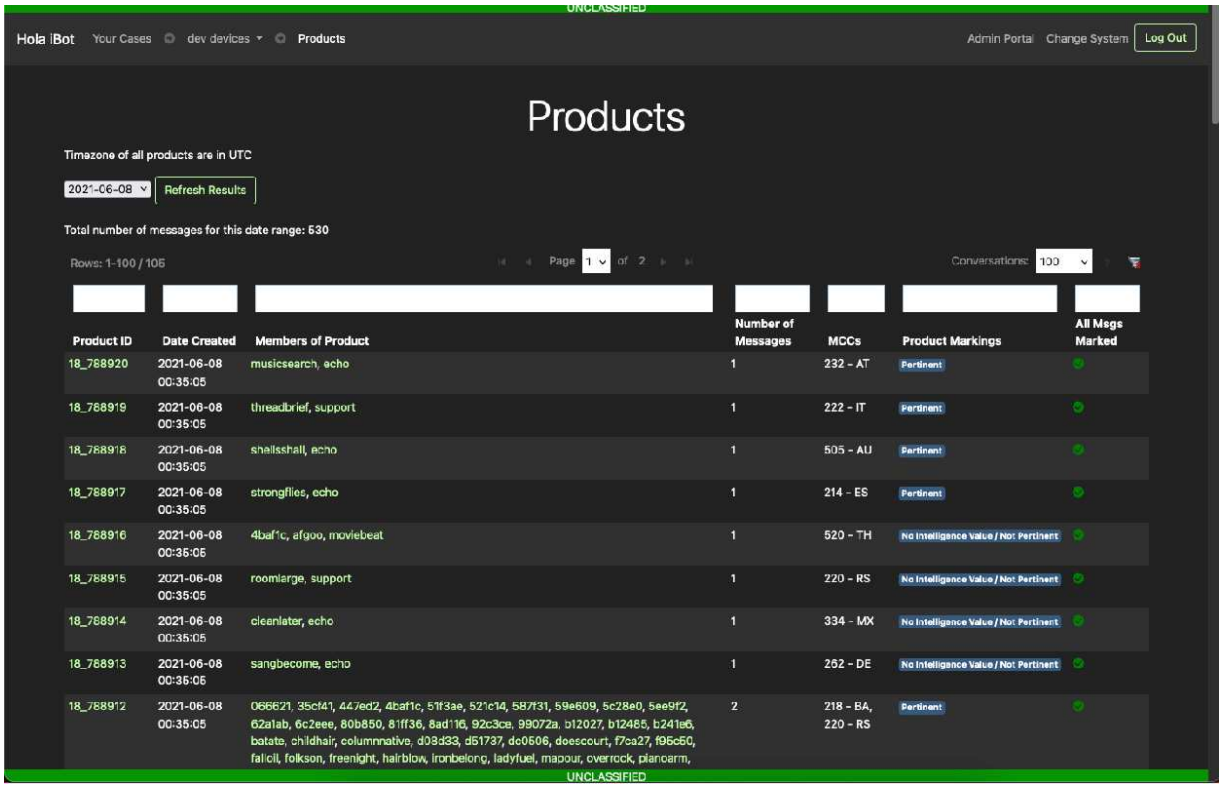
Skärmbild 10.E

I resten av avsnitt 10 beskrivs alternativen på ärendets hemsida närmare.

10.3 Produktsidan

Produktsidan är den sida som användare går till för att visa konversationerna i ärendet. Se avsnitt 8.5 för mer information om produkter och avsnitt 9.4 för mer information om hur produkter skapas.

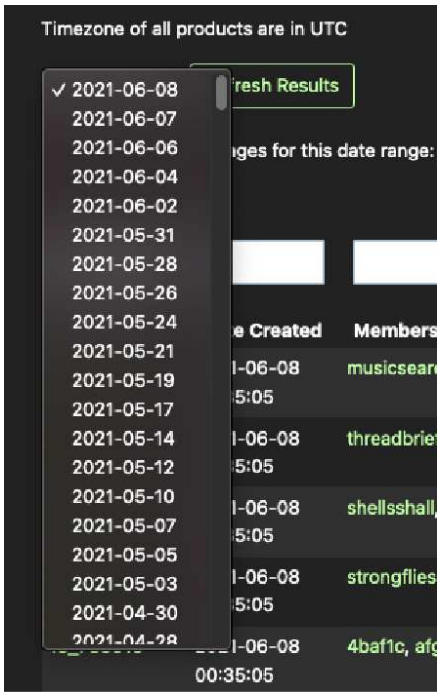
Produkter är unika konversationer för ett ärende som togs emot i ett datapaket. I skärmbild 10.F visas produktsidan för ärendet ”dev devices”.



Skärmbild 10.F

I nedrullningsmenyn överst till vänster där ”2021-06-08” är ifyllt finns en lista med datum då nya

datapaket togs emot:



Skärmbild 10.F.1

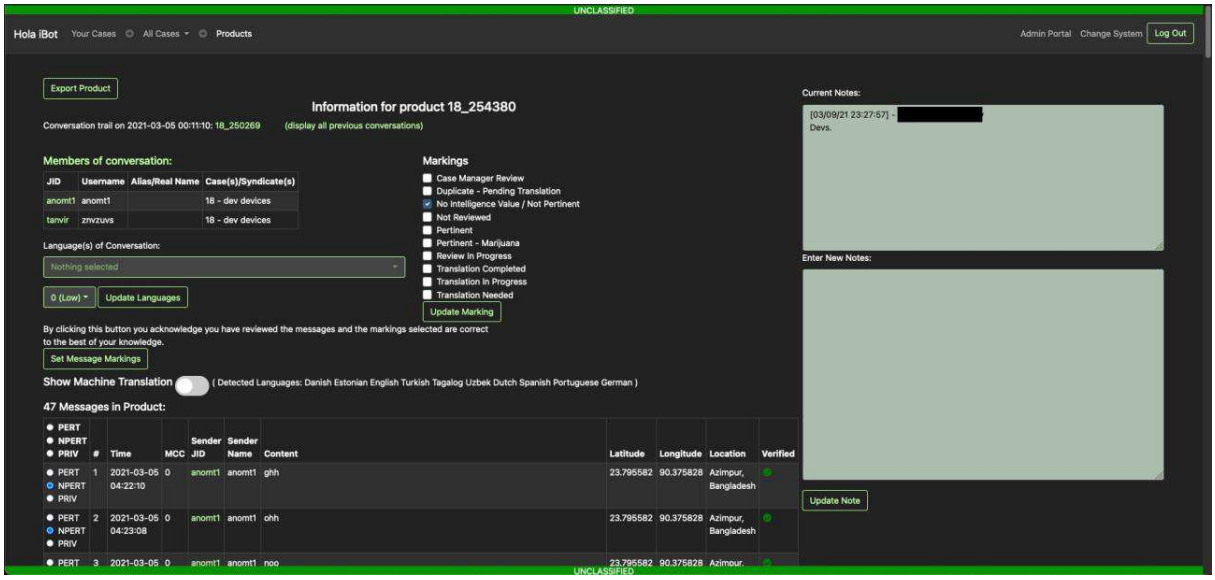
Listorna med produkter är unika per överföringsdatum. Som visas i skärmbild 10.F visas inte produkt-ID (PID) under ”Product ID” i listan över produkter. Det ”Product ID” som visas för användaren anges med ärende-ID följt av understreck och sedan det faktiska produkt-ID:t (PID). Det är ett enklare sätt att universellt hänvisa till produkter och det blir enklare att veta vilka ärenden som produkten hör till.

Resten av data som visas på den här sidan hämtas från tabellerna ”produkter”, ”har_markering” och ”har_meddelande”.

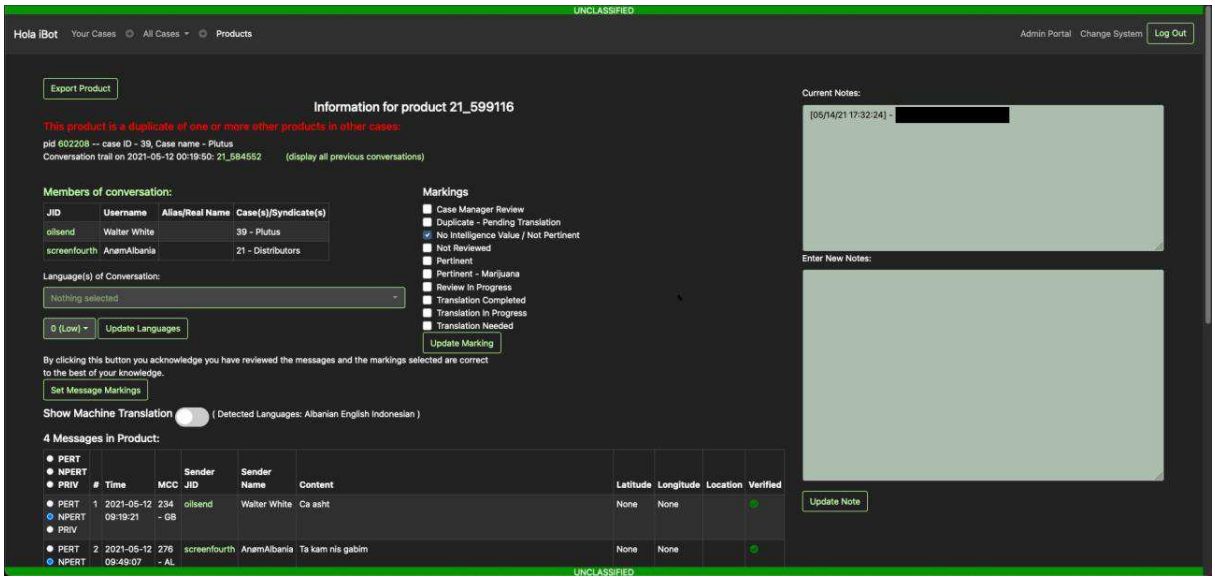
- “Date Created”
  - hämtas från fältet för skapandedatum i tabellen ”produkt”
- ”Members of Product”
  - hämtas från fältet ”JID-sträng” i tabellen ”produkt”
  - Alla JID:n som visas i den här kolumnen är länkade till JID-profilen.
    - Se avsnitt 10.7 för mer information om JID-profilen.
- ”Number of Messages”
  - hämtas från fältet ”antal” i tabellen ”produkt”
- ”MCCs”
  - hämtas från fältet ”MCC-sträng” i tabellen ”produkt”
- ”Product Markings”
  - hämtas från tabellen ”har_markering”, som relaterar produkten till en textbaserad markering
- ”All Msgs Marked”
  - hämtas genom att köra en sökfråga mot tabellen ”har_meddelande” för att testa om alla meddelanden har en markering som inte är standard

10.4 Produktsidan

Länkarna under ”Product ID” går till produktsidan, där meddelandena för produkten visas som på skärmbild 10.G och 10.G.1.



Skärmbild 10.G



Skärmbild 10.G.1

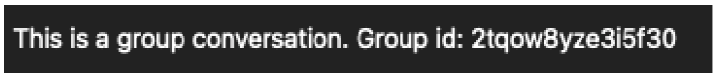
På produktsidan visas många olika typer av information för användaren av granskningsplattformen. Produktsidan visar följande information (se skärmbild 10.G och 10.G.1):

- Huruvida produkten som visas är en dubblett av en produkt i ett annat ärende.
    - I skärmbild 10.G.1 visas ett exempel på en produkt som är en dubblett, och där finns också en länk till den motsvarande dubbletten.
- Deltagarna i konversationen
    - Dessa sammanställs under inmatningsprocessen som beskrivs i avsnitt 9.4.1.1.
- De språk som granskningsplattformens användare har lagt till för produkten.

    - Flera språk kan läggas till i listan.
    - Språklistan motsvarar inlämnade översättningar.
        - Mer information finns i avsnitt 10.5.1.
- De markeringar som har lagts till för produkten
- De meddelandemarkeringar som granskningsplattformens användare har ställt in
- Anteckningar som har skapats om produkten (höger ruta).
    - När en anteckning väl har skapats kan den inte tas bort, utan den flyttas istället till rutan ”Current Notes” med en tidsstämpel som visar när den skapades samt användarnamnet för den användare av granskningsplattformen som lade till anteckningen.
    - Dessa anteckningar motsvarar fältet ”produktanteckning” i tabellen ”produkter”.
- Alla översättningar som har lagts till i produkten baserat på det språk som lades till syns längst ned på produktsidan.

10.4.1 Grupp-ID-visning

Om produkten motsvarar en grupp kommer följande att visas om det finns gruppinformation i databasen iBot_dec:



Skärmbild 10.G.2

10.4.2 Meddelanden med bilagor (PTT, bild, video, anteckning) i Hola iBot

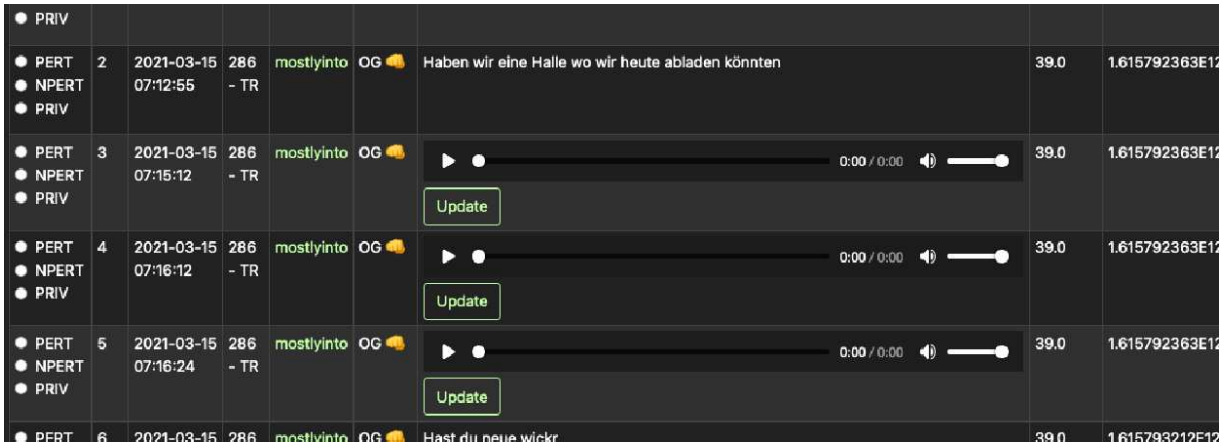
Alla meddelanden med bilagor visas inline, som textmeddelanden. Meddelanden med bilagor kan också ha en markering som tilldelas av användare av granskningsplattformen. I databasen iBot_dec finns en tabell med namnet ”bilaga_har_markering” som gör det möjligt att markera bilagor med textbaserade beskrivningar. Tabellen ”bilaga_har_markering” innehåller följande Fält:

- Meddelande-ID (MID)
    - Det MID som den textbaserade beskrivningen motsvarar
- Markering
    - Den textbaserade beskrivningen av markeringen

Markeringarna av bilagor kan ställas in på produktsidan av granskningsplattformens användare.

10.4.2.1 PTT-meddelanden (push-to-talk) i Hola iBot

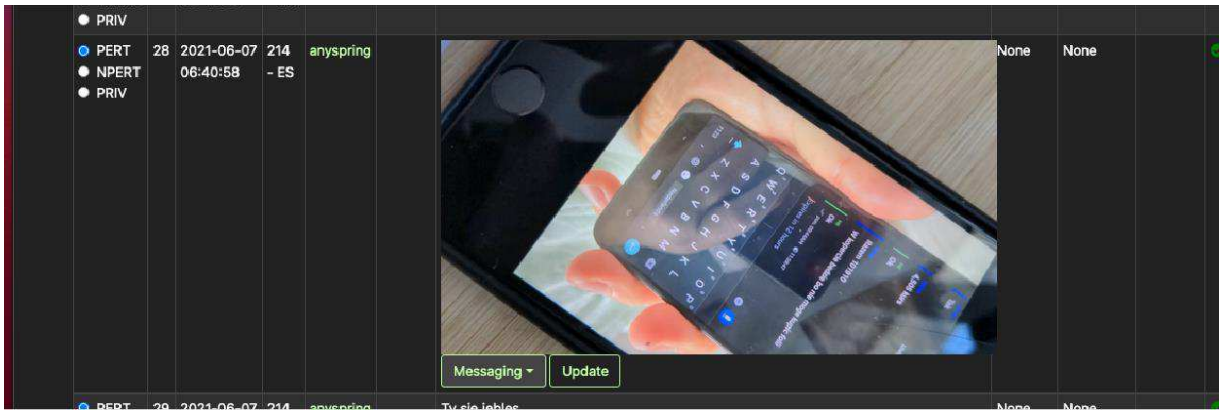
I skärmbild 10.G.3 visas ett exempel på några PTT-meddelanden.



Skärmbild 10.G.3

10.4.2.2 Bildmeddelanden i Hola iBot

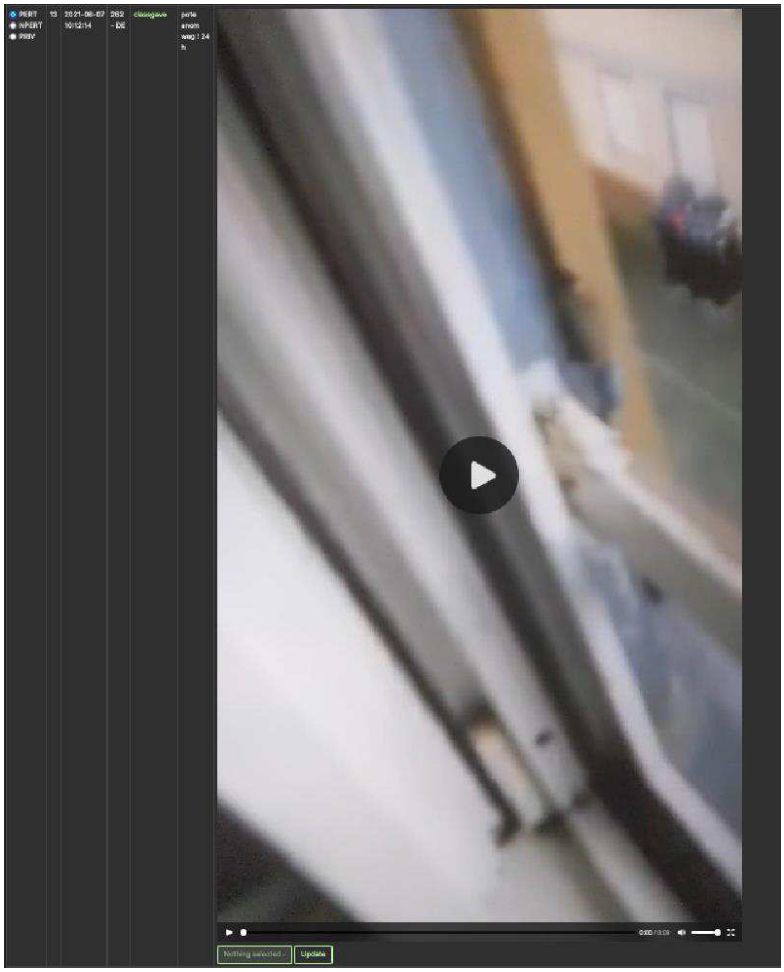
I skärmbild 10.G.4 visas ett exempel på ett bildmeddelande som visas inline.



Skärmbild 10.G.4

10.4.2.3 Videomeddelanden i Hola iBot

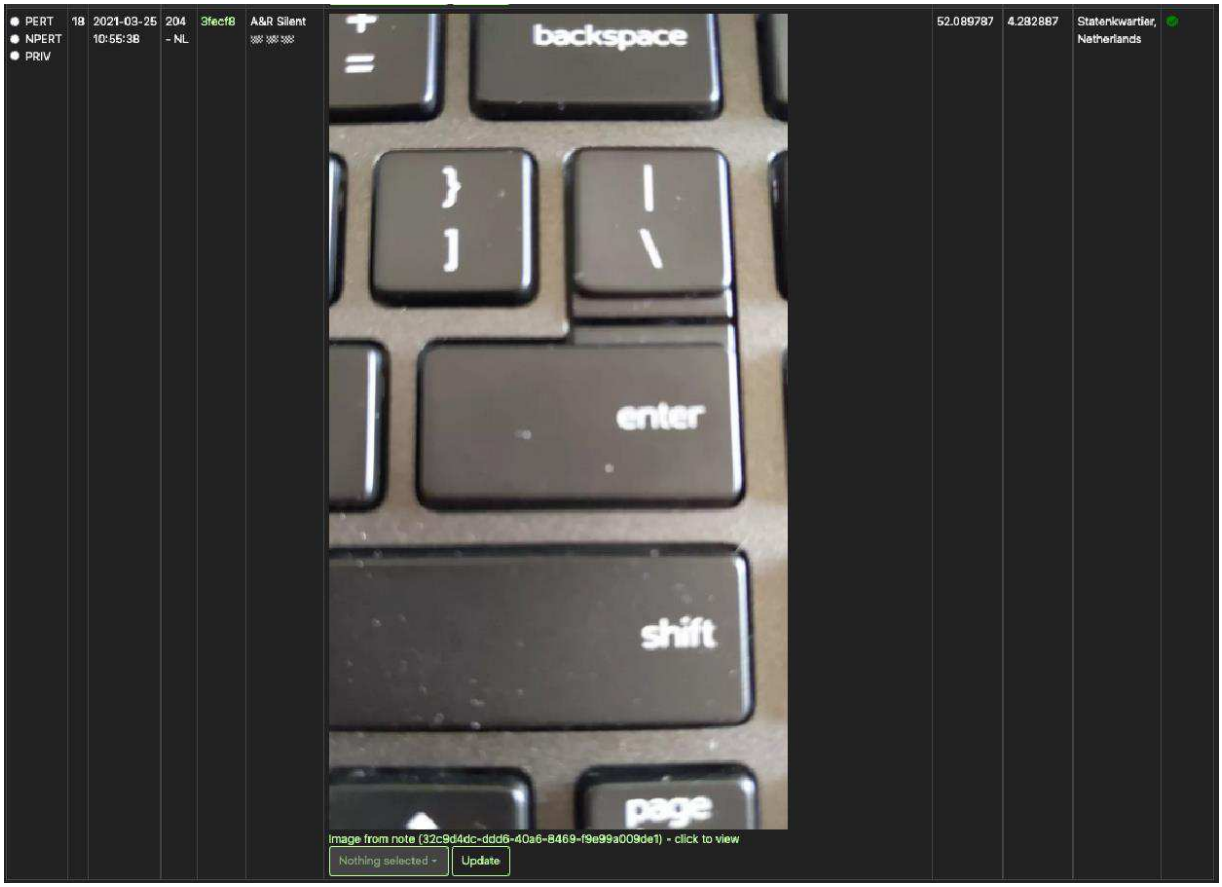
I skärmbild 10.G.4 visas ett exempel på ett videomeddelande i Hola iBot.



Skärmbild 10.G.5

10.4.2.4 Anteckningsmeddelanden i Hola iBot

I skärmbild 10.G.6 visas ett exempel på en bildkomponent för en anteckning som visas inline som ett meddelande.



Skärmbild 10.G.6

Texten ”Image from note ([Original Message ID]) – click to view” anger att bilden kommer från ett anteckningsmeddelande.

10.5 Översättningar

Om en produkt har tilldelats ett språk med hjälp av nedrullningsmenyn i skärmbild 10.G och 10.G.1 skickas produkten automatiskt på översättning. På grund av de många-till-många-relationer som språk har med produkter finns en tabell med namnet ”har_språk” i databasen för att skapa dessa relationer. Tabellen ”har_språk” har följande attribut:

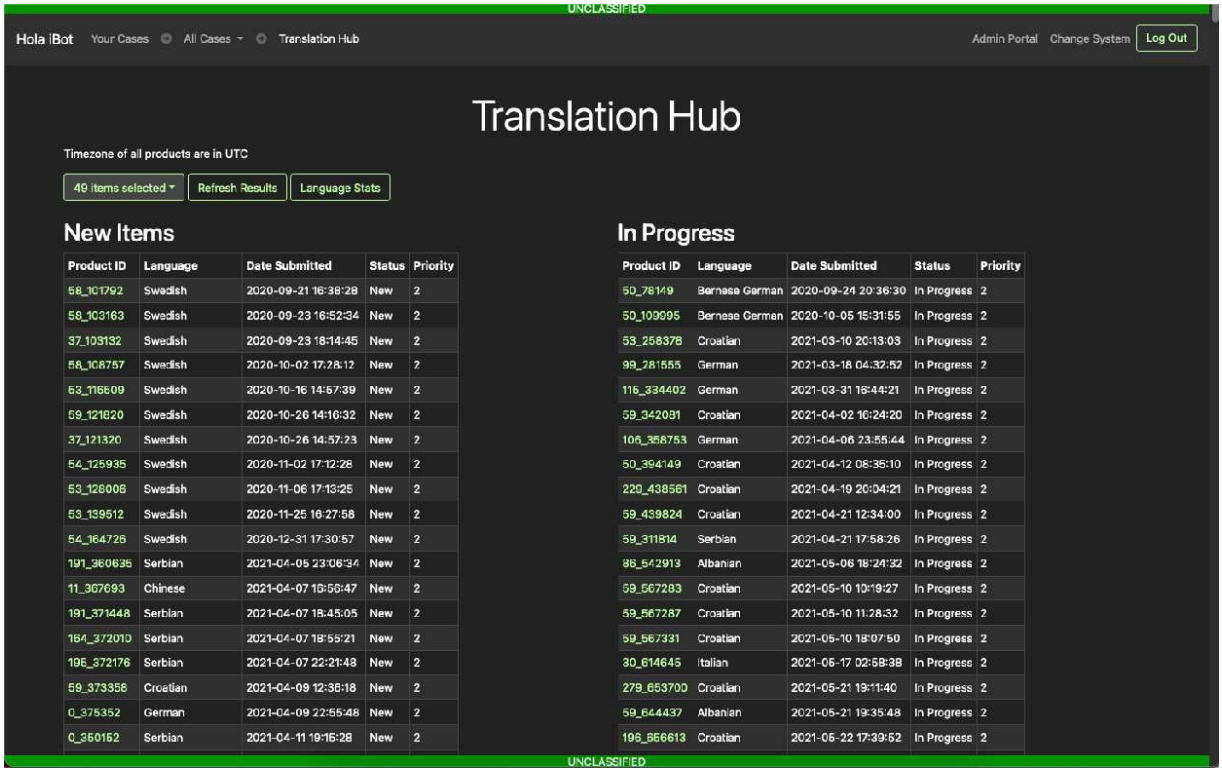
- Språk
  - Namnet på språket som tilldelas till produkten.
  - Exempel: ”engelska”, ”spanska”
- Produkt-ID (PID)
  - PID för den produkt som språket tilldelas till.
- Status
  - Det här fältet visar status på översättningen.
  - Det här fältet kan anges till ”ny”, ”pågående” eller ”klar”.
- Prioritet

- Det här fältet anger prioritet på översättningsbegäran.
- Inskickad av
  - I det här fältet anges det användarnamn på granskningsplattformen som lade till språket i produkten.
- Översättning
  - Det här är det värde som lingvisterna anger för översättningen av produkten.
- Datum för inskickande
  - Anger det datum då språket lades till för produkten
- Ärende-ID
  - Det ärende-ID som produkten motsvarar i raden av värden
- Färdigställd av
  - Det användarnamn i granskningsplattformen som angav fältet ”status” till ”klar”

När ett språk har lagt till för en produkt går det att visa produkt-ID, ärende-ID och språknamn på sidan Translation Hub.

10.5.1 Translation Hub

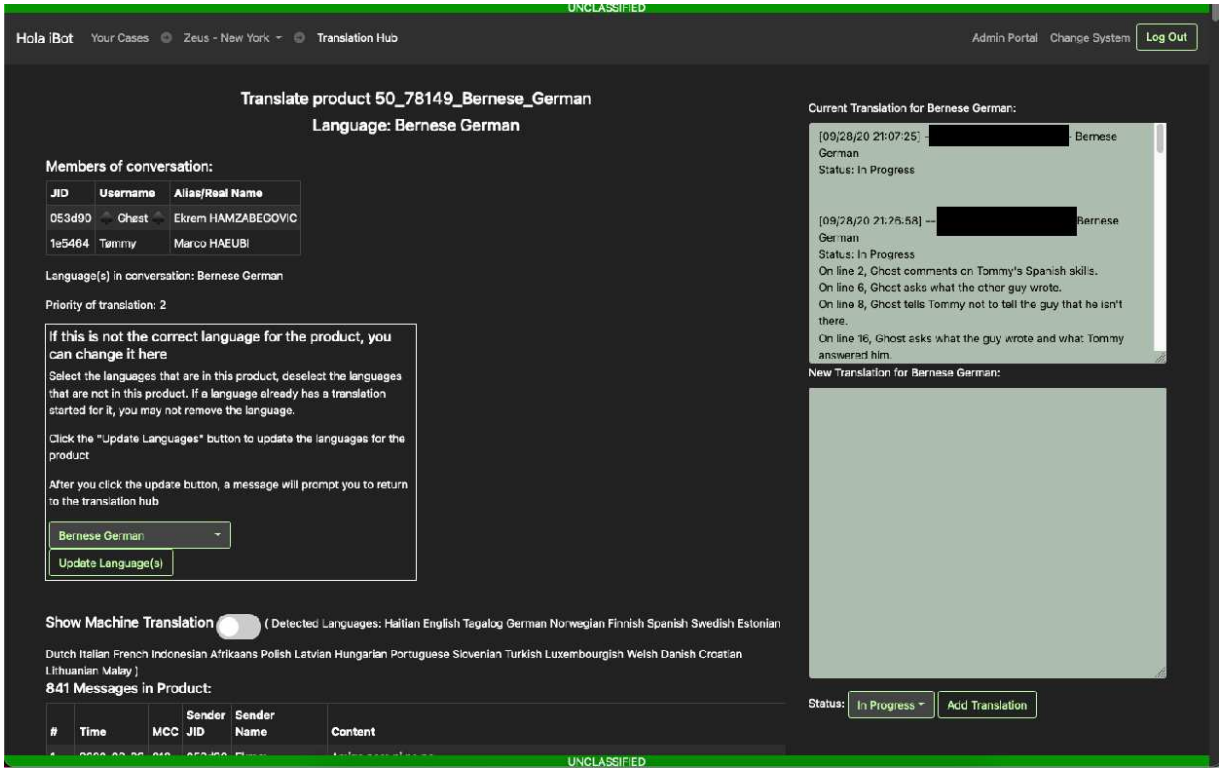
I Translation Hub finns alla översättningar som har lämnats in av användare för produkter. Skärmbild 10.H visar Translation Hub.



Skärmbild 10.H

De två listorna visar status från tabellen ”har_språk” för motsvarande produkt-ID (PID). Om en översättningsförfrågan i tabellen ”har_språk” har statusen ”klar” visas den inte längre i de två listorna.

Efter att ha klickat på en länkad produkt i Translation Hub visas en sida som liknar produktsidan, se skärmbild 10.I.



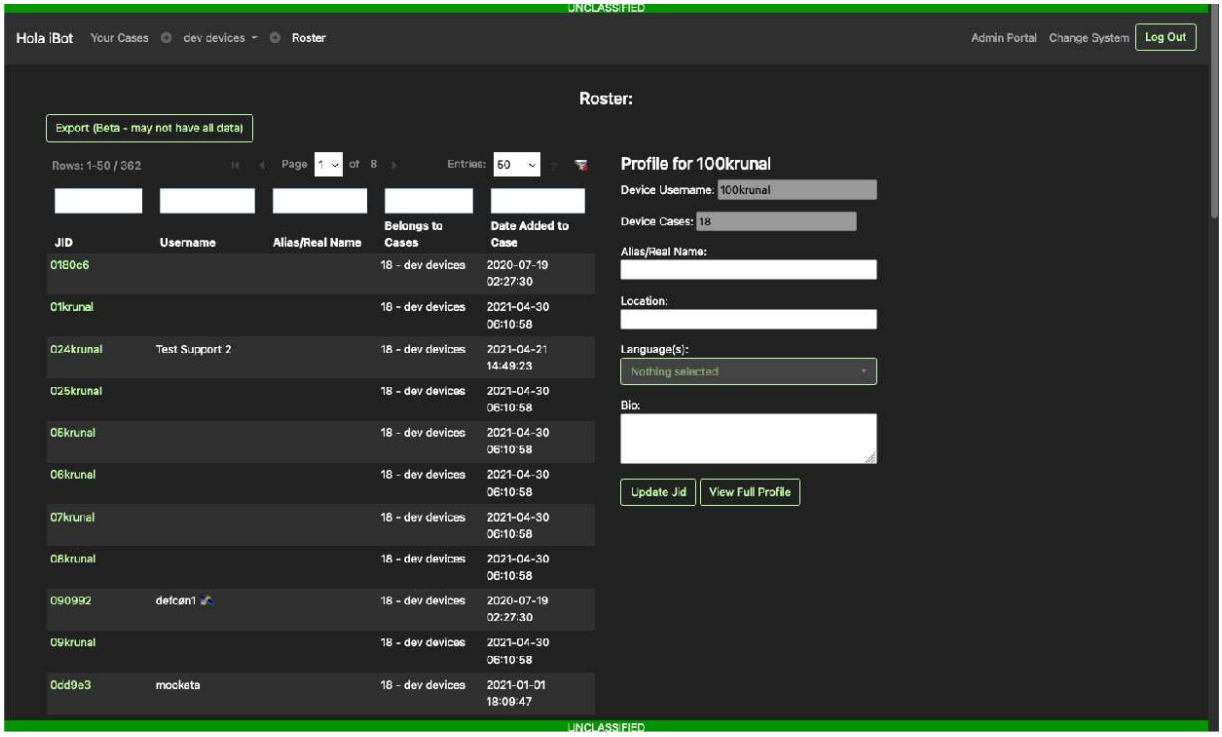
Skärmbild 10.I

På den här sidan lägger översättare till översättningar av produkter. I rutan till höger i skärmbild 10.I kan användare lägga till översättningar. När en översättning läggs till fungerar det som när en användare av granskningsplattformen lägger till anteckningar i produkter. De flyttas till textrutan ”Current Translation for [namn på språket]”. Översättningar som redan har skickats in och flyttats till den andra rutan kan inte uppdateras. De loggas också med en tidsstämpel och användarnamnet för den användare av granskningsplattformen som lade till översättningen.

Alla anteckningar som har lagts till för motsvarande produkt via produktsidan visas längst ned på översättningssidan.

10.6 Förteckningssidan

Sidan som visar förteckningen visar en lista med enhetsanvändare (JID) som har en relation med ett ärende i tabellen ”tillhör”. I skärmbild 10.J visas ett exempel på en förteckningssida för ärendet ”dev devices”.



Skärmbild 10.J

Sidan är delad vertikalt i två rutor.

I den vänstra rutan visas listan med enhetsanvändare (JID) med deras användarnamn (enhetsanvändarnas visningsnamn), verkligt namn (angett av granskningsplattformens användare om det har uppdagats under utredningen), motsvarande ärenden (enligt tabellen ”tillhör”) och datumet då de lades till i ärendet (enligt tabellen ”tillhör”).

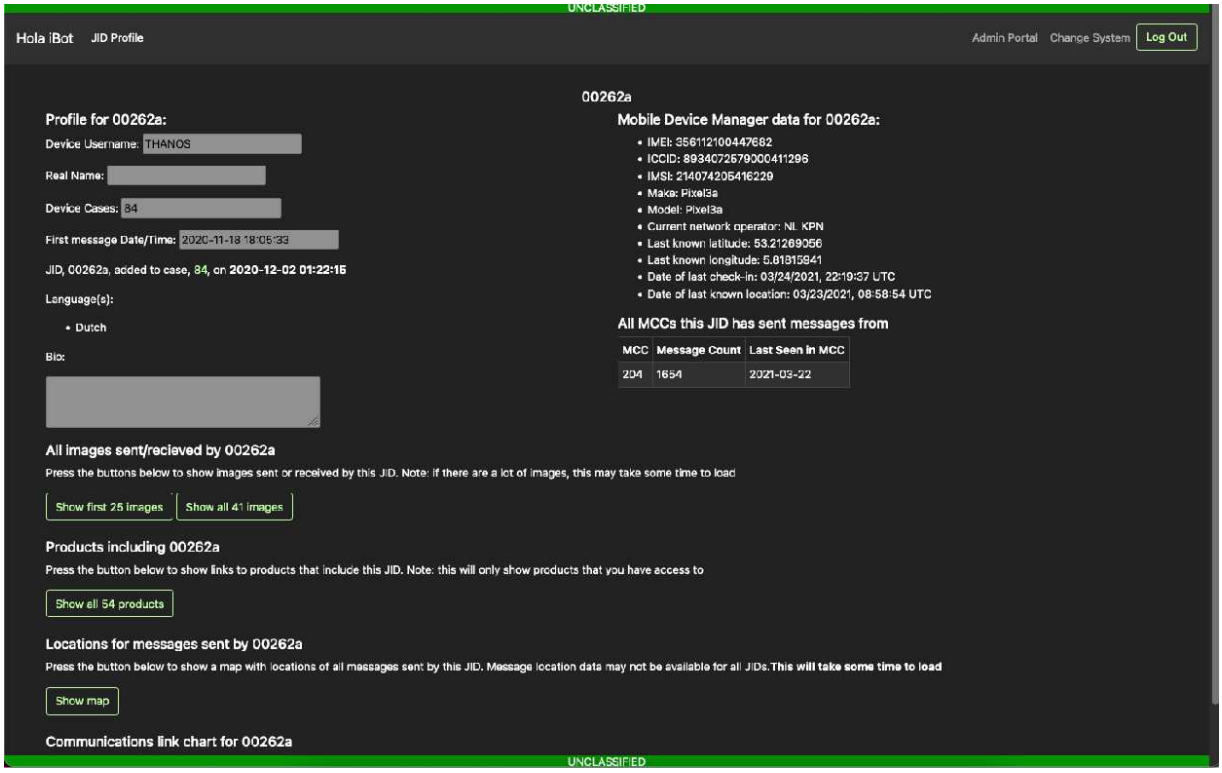
Det går att klicka på varje rad i tabellen och då fylls den högra rutan på med följande ytterligare information, som kan redigeras:

- Alias/verkligt namn
- Plats
- Språk
- Biografi

I avsnitt 8.3 finns mer information om fälten i förteckningen.

10.7 JID-profil

Det går att länka till JID-profilen från ett antal olika sidor. Ett exempel på en JID-profil visas i skärmbild 10.K.



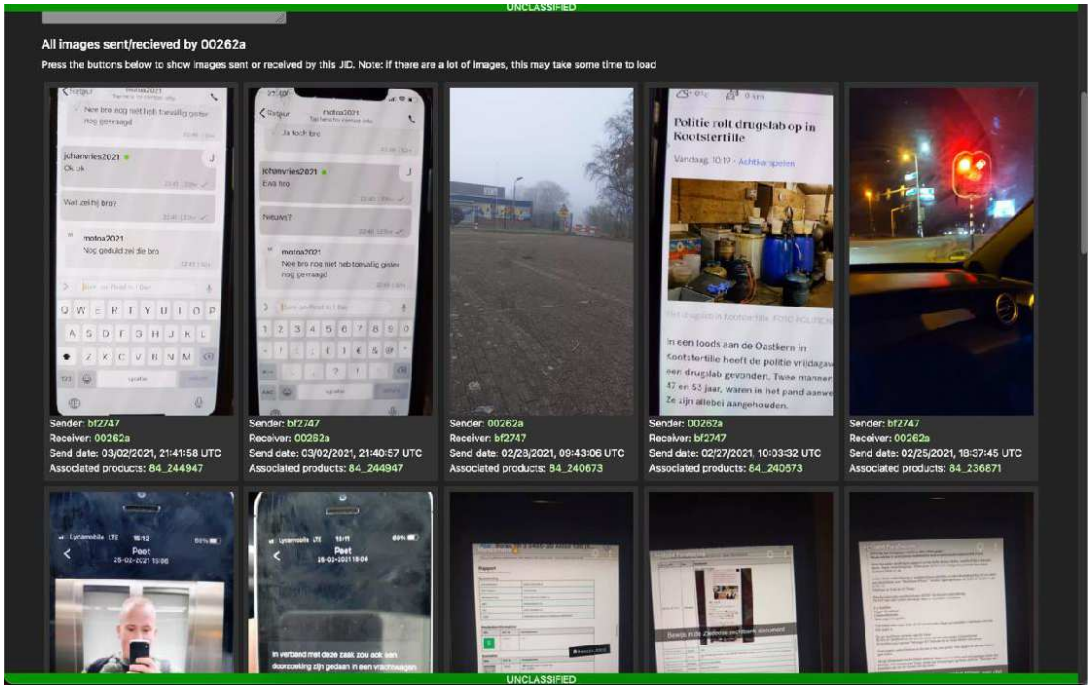
Skärmbild 10.K

Resten av avsnitt 10.7 hänvisar till skärmbild 10.K.

10.7.1 Information om enhetsanvändaren (JID)

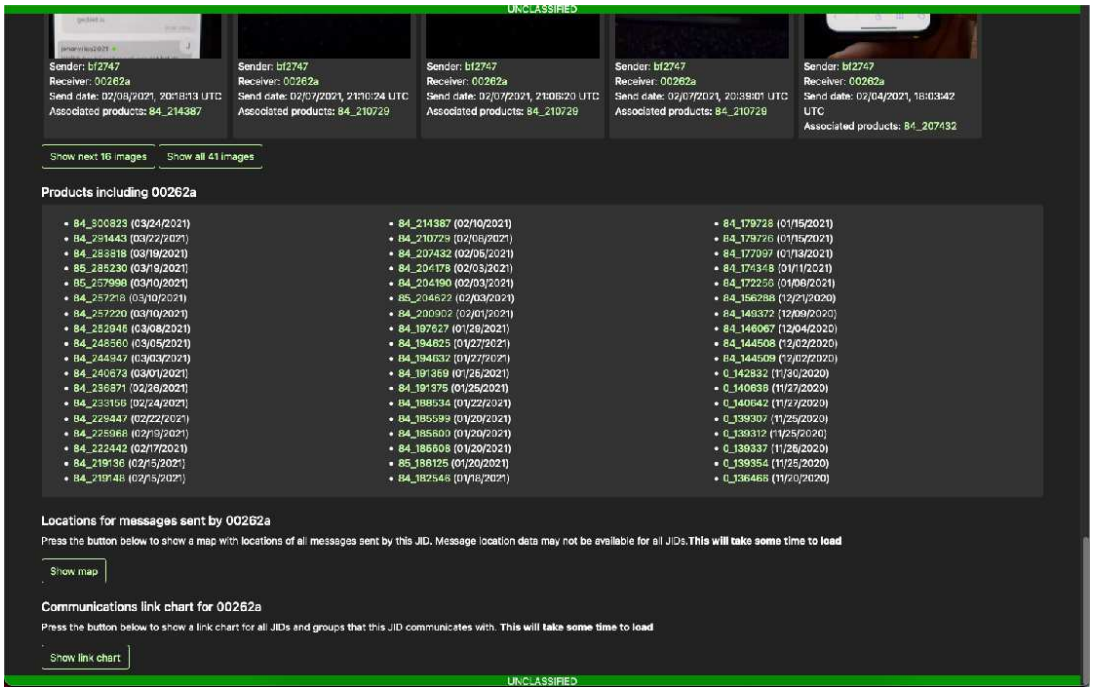
Alla förteckningsdata om enhetsanvändaren (JID) visas på JID-profilsidan. Det finns andra data som också kan hämtas från JID-profilsidan, t.ex.:

- Bilder som har skickats av enhetsanvändaren.
  - ”All images sent/received by 00262a” i skärmbilden.



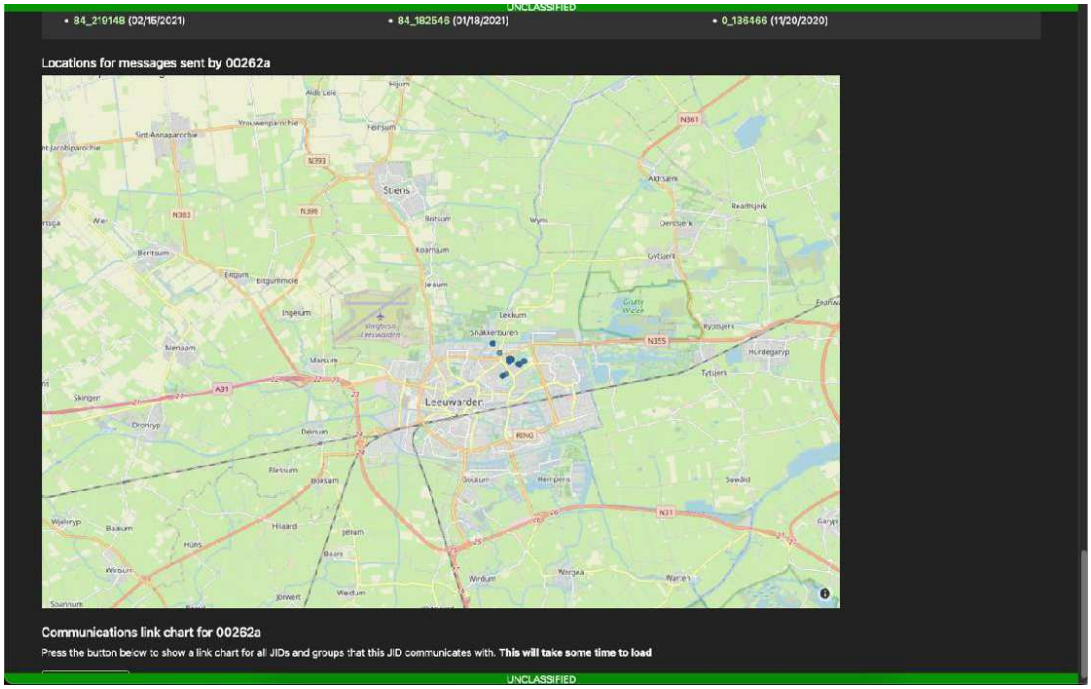
Skärmbild 10.K.1

- Produkter som användaren skickade eller tog emot meddelanden i.
  - "Products including 00262a" i skärmbilden.



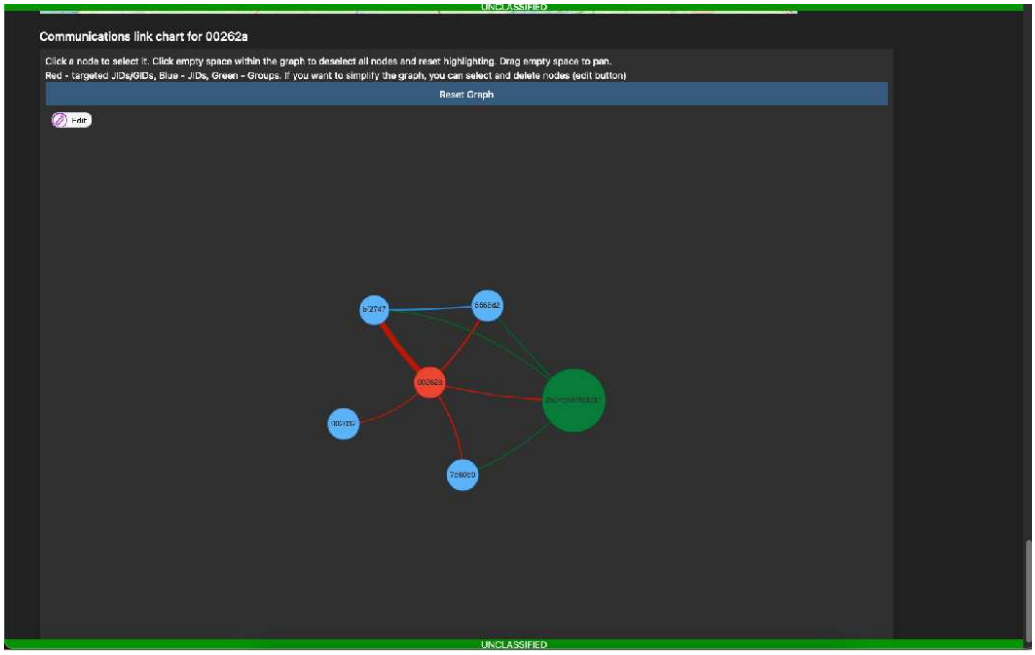
Skärmbild 10.K.2

- Om GPS-data för meddelanden var tillgängliga visas de. Mer information finns i bilaga A, 8.2.
  - ”Locations for messages sent by 00262a” i skärmbilden.



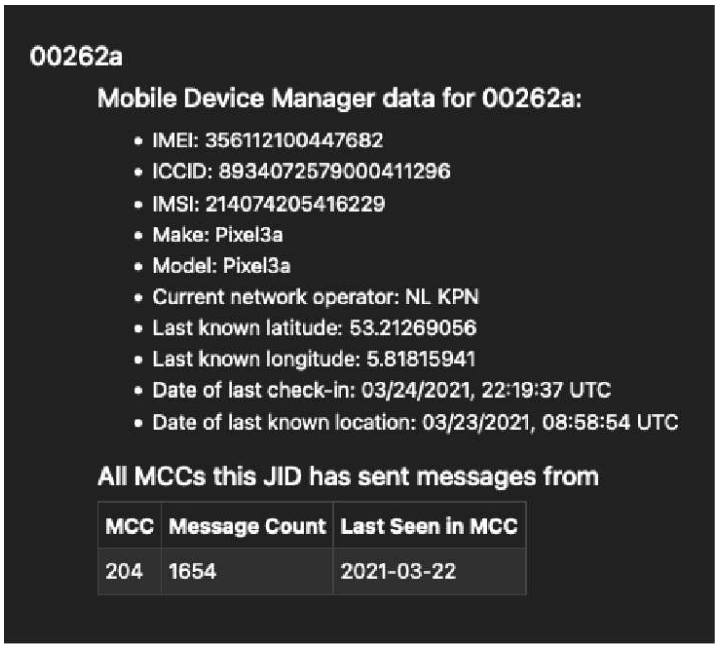
Skärmbild 10.K.3

- En interaktiv kommunikationskarta med länkar.
  - ”Communications link chart for 00262a” i skärmbilden.
  - Om man hovrar över en nod visas JID för avsändaren, ärende och senaste MCC.
  - Om man dubbelklickar på noden skickas användaren av granskningsplattformen till JID-profilen för den valda noden.



Skärmbild 10.K.4

- MDM-information (Mobile Device Manager)
  - Enligt beskrivningen i bilaga A.5 – 24.a hanterades ANØM-plattformen av en MDM-applikation, och en del av informationen från MDM-portalerna matades in i databasen iBot_dec i syfte att tillhandahålla ytterligare information om enhetsanvändare.
  - I skärmbild 10.K.5 visas en förstorad skärmbild av MDM-data för JID:t i skärmbild 10.K.



Skärmbild 10.K.5

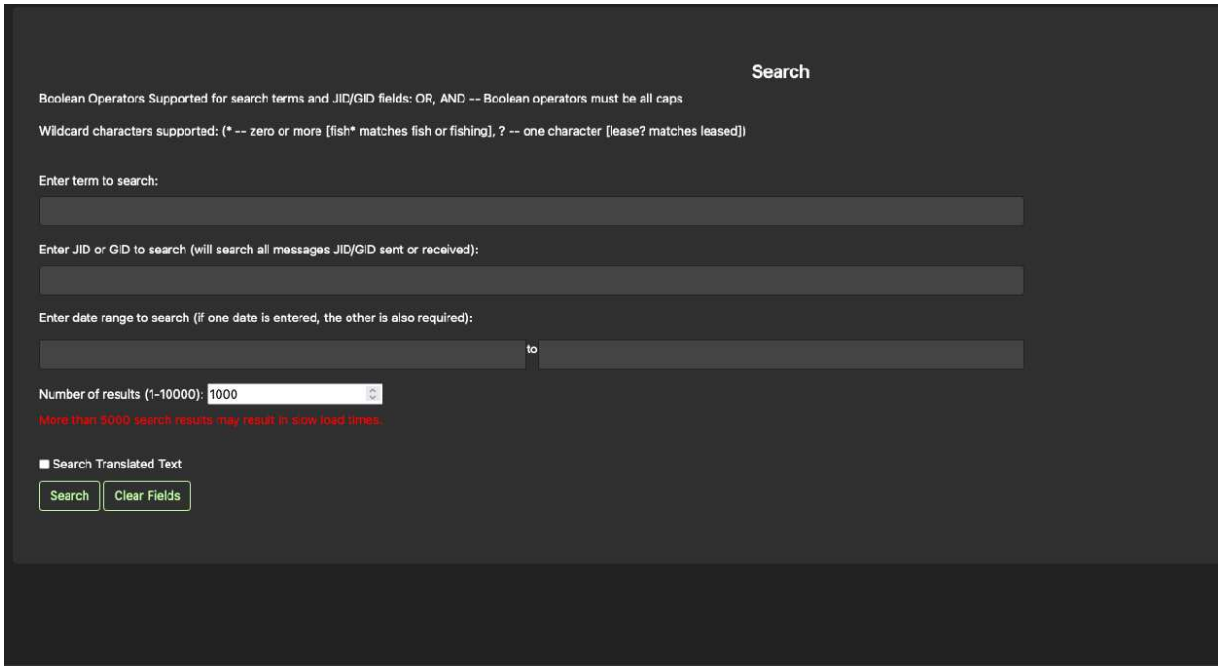
10.8 Andra sidor

10.8.1 Sökning

På söksidan kan man söka i:

- fältet ”innehåll” för meddelanden.
- enhetsanvändar-ID (JID).
- grupp-ID (GID).

Det går också att ange datumintervall för att filtrera resultaten.



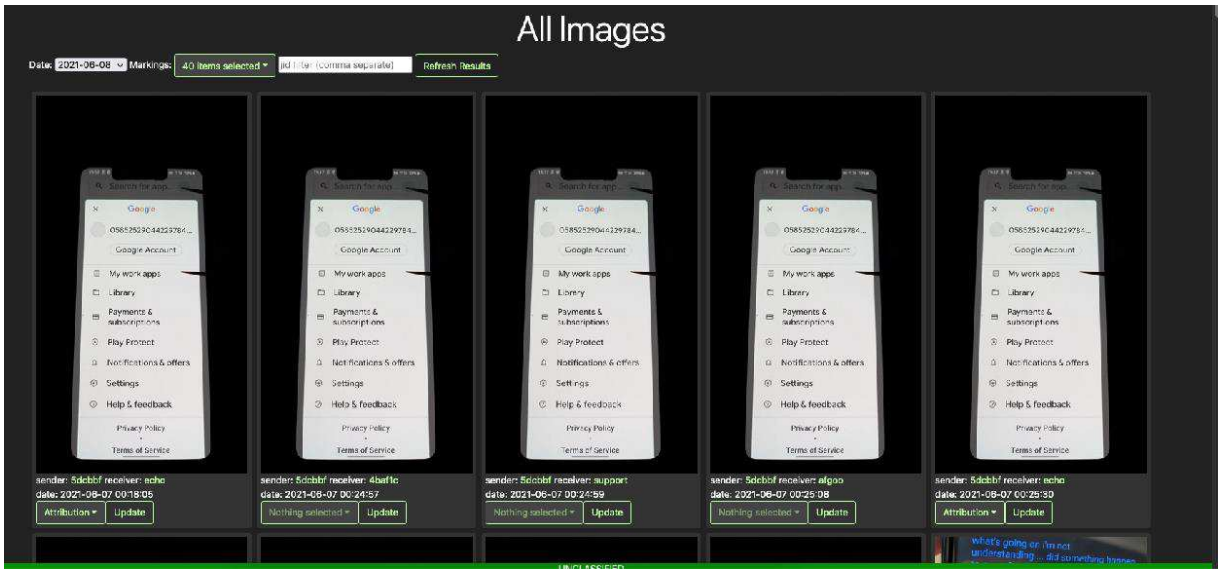
Skärmbild 10.L

10.8.2 Sök i anteckningar

När användare av granskningsplattformen lägger till anteckningar blir de sökbara via sidan Sök i anteckningar. Den har ett gränssnitt som liknar söksidan.

10.8.3 Alla bilder

På sidan Alla bilder visas alla bilder inom ramen för nuvarande åtkomstkontroller, och det går att bläddra igenom dem, markera dem med bilagemarkeringar och visa dem.



Skärmbild 10.M

10.8.4 Blockerade

En lista med meddelanden som blockerades enligt beskrivning i 9.3.1.1. Mer information kommer i en framtida bilaga.

Alla andra navigerbara sidor, baserat på användarroll (se avsnitt 8.2), används av granskningsplattformens administratörer och för andra utredningssyften.

11. MLAT-EXPORT

MLAT-förfrågningar hanteras av FBI:s field office i San Diego. De skickas in av olika länder för en lista med enhetsanvändare (JID). Förberedelser gjordes för MLAT-förfrågningarna genom att flera steg vidtogs för att skapa en automatiserad process som kunde exportera data på ett säkert sätt.

11.1 Hämtning av alla bifogade filer

Ett steg i förberedelserna var att hämta alla bifogade filer från I1-servern i AWS GovCloud. Dessa bifogade filer lagras på en arbetsstation på FBI:s field office i San Diego, som kan skapa automatiska exporter.

11.2 Hämtning av slutlig MySQL-databasdump

När nya datapaket färdigställdes den 08.06.2021 skapades en fullständig MySQL-databasdump som hämtades inför skapandet av exporter. Tidsstämplar för alla exporterade meddelanden anges i tidszonen Pacific Time.

11.3 Skapa MLAT-exporter

En sökning görs i databasen, enligt en lista på enhetsanvändare (JID), efter alla meddelanden som har skickats eller mottagits och som är relevanta för enhetsanvändaren. Meddelandena lagras tillfälligt i en andra databas som kopieras in i en .sql-fil som bifogas svaret på förfrågan. Den innehåller också alla konversationer med efterfrågade JID:n oavsett vilket syndikat (ärende) de är placerade i.

En extern enhet förbereds med LUKS-kryptering och ett lösenord som skickas i förväg till de som skickade MLAT-förfrågan. .sql-filen kopieras till den krypterade enheten tillsammans med en lista på de enhetsanvändare (JID) som efterfrågades.

Listan med bifogade filer sparas till en fil medan data bearbetas och den filen går igenom en andra process som kopierar varje bifogad fil till den krypterade enheten.

Efter att stegen som beskrivs i det här avsnittet har gåtts igenom är MLAT-exporten klar och kan skickas till det begärande landet.

BILAGA A

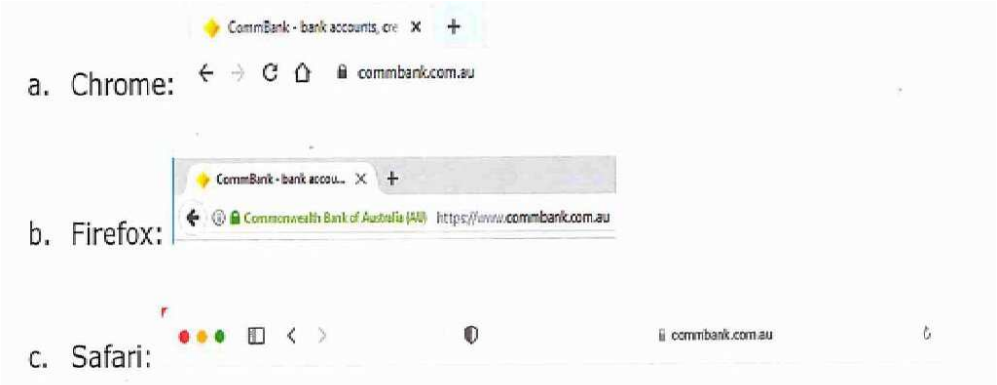
A.1 Kryptering med offentlig nyckel

1. Kryptering innebär att information kodas så att den inte kan läsas av någon som saknar medlen för att avkryptera den. Kryptering med offentlig nyckel är en krypteringsmetod där två olika nycklar, den ”offentliga” och den ”privata”, används för att kryptera och avkryptera information. De två nycklarna hör ihop matematiskt så att information som har krypterats med den ena bara kan avkrypteras med den andra. Samma nyckel kan inte användas till att kryptera och sedan avkryptera samma information. Det innebär att information som har krypterats med den offentliga nyckeln är säker så länge som den privata nyckeln är skyddad. Den är oläslig för alla som inte har den privata nyckeln.

2. Kryptering med offentlig nyckel har många tillämpningsområden och är vanligt på internet. TLS (Transport Layer Security) är ett exempel på kryptering med offentlig nyckel.

3. TLS är en ofta använd säkerhetsmekanism som skyddar data som skickas till många webbplatser. Om den används visas ett litet hänglås i webbläsarens adressfält. Hänglåset kan ofta ses på webbplatser som tillhör t.ex. banker, webbaserad e-post och Google, vilket gör att användare kan vara säkra på att informationen som de skickar till webbplatsen är säker. Den här formen av transportsäkerhet gör också att data som skickas mellan en server och en klient inte kan avlyssnas av en tredje part under överföringen. Alla webbplatser som du besöker där hänglåsikonen visas i adressfältet på webbläsaren använder kryptering med offentlig nyckel för att skydda dina data.

4. Exempel på hur hänglåsikonen visas på webbplatsen för Commonwealth Bank of Australia i webbläsarna Chrome, Firefox och Safari:



5. Eftersom kryptering med offentlig nyckel kräver mycket processorkraft används den i allmänhet inte för att kryptera stora mängder data. Ett annat alternativ är att använda en symmetrisk nyckel, den så kallade sessionsnyckeln i TLS, för att kryptera data och sedan använda kryptering med offentlig nyckel för att kryptera själva nyckeln. Den krypterade nyckeln infogas sedan i krypterade data. Innehavaren av den privata nyckeln kan sedan avkryptera den symmetriska nyckeln och använda den till att avkryptera data.

A.2 Hash

6. En ”hashfunktion” är ett matematiskt förhållande där indata av godtycklig storlek” (det så kallade ”meddelandet”) bearbetas till utdata med fast storlek (”sammandrag av meddelande” eller ”hashvärde”). Vissa hashfunktioner kan användas för kryptering. Bland dessa finns algoritmfamiljen Secure Hash Algorithm 2 (”SHA-2”) som utvecklades av USA:s National Security Agency and publicerades av USA:s Department of Commerce som en del av

FIPS (Federal Information Processing Standards). De är offentligt tillgängliga på internet.

7. SHA-2-algoritmerna kan användas för att verifiera integriteten för data (däribland datorfiler) eftersom det är väldigt osannolikt att två olika meddelanden ger samma hashvärde som utdata. Det gäller även om ett meddelande har förändrats, vilket ger ett annorlunda meddelande. Det här förklaras i FIPS Publication 180-4:

   > *De hashalgoritmer som specificeras i den här standarden betecknas som säkra eftersom det, för en algoritm, är matematiskt omöjligt att 1) hitta ett meddelande som motsvarar ett visst hashvärde eller 2) hitta två olika meddelanden som resulterar i samma hashvärde. Alla förändringar av ett meddelande kommer med mycket hög sannolikhet att resultera i ett annat hashvärde. Det i sin tur leder till att verifieringen misslyckas...*

8. Algoritmen MD5 (Message Digest 5) anses inte längre lämplig för krypteringsändamål, men den används ofta för sådana syften som att skapa checksum-värden för att kontrollera att data inte oavsiktligt har blivit korrupta. Den representeras ofta med 32 hexadecimala tecken (siffrorna 0 till 9 och bokstäverna A till F).

9. En hash är konstruerad för att vara en irreversibel process, eftersom den producerar ett hashvärde med fast längd för meddelandeindata av en given längd. En enkel liknelse är att ta summan av två tal (t.ex. 23 + 78 = 101). Det är extremt svårt att fastställa exakt vilka två tal som användes för att komma fram till utdata (101), men det går att arbeta sig igenom varenda tänkbar kombination för att identifiera de kombinationer som ger den summan. Processen kallas ”brute force” och varje hittad kombination är en ”hash-kollision”. Om ekvationen som gav summan görs ännu mer komplicerad – t.ex. genom att man använder multiplikation, subtraktion och division förutom den ursprungliga additionen – skulle det bli mycket svårare och ta längre tid att identifiera sifferkombinationerna. Det skulle också leda till en mindre underuppsättning av tänkbara ursprungliga indatavärden.

10. Eftersom hashfunktionerna är så komplicerade ägnar matematiker och kryptoanalytiker mycket tid åt att försöka omvända funktionen för att bevisa att det verkligen är en envägsfunktion. Det enda sättet att identifiera ett ursprungligt indatameddelande från ett hashvärde är därmed att genomföra en brute force-process, och det är en alltför komplicerad uppgift för att vara praktiskt genomförbar.

A.3 ANØM-PLATTFORMEN

11. Kommunikationsnätverket ANØM ger end-to-end-kryptering av meddelanden i ett slutet nätverk mellan ANØM-användare. Att nätverket är slutet innebär att den end-to-end-krypterade kommunikationen bara kan ske mellan ANØM-användare. Det är en prenumerationsbaserad tjänst som kräver att man köper smartphones som är särskilt konfigurerade att kommunicera på ANØM, och bara telefoner som har konfigurerats på rätt sätt kan användas för kommunikationen.

12. FBI anlitade tredje parter för att konfigurera och driva ANØM, inklusive att vara primärt ansvariga för att utveckla applikationen samt att hantera och underhålla infrastrukturen för funktionerna i ANØM (ANØM-administratörer).

A.3.1 End-to-end-kryptering

13. End-to-end-kryptering är en typ av kryptering där meddelandenas innehåll bara kan läsas av de parter som deltar i kommunikationen, och ofta används kryptering med offentlig nyckel i sådana sammanhang.

14. Med end-to-end-kryptering säkerställer man att innehållet i det ursprungliga

meddelandet inte kan läsas av leverantören av meddelandetjänsten eller någon annat system eller nätverk från tredje part som meddelandet skickas genom. Meddelandetjänster med end-to-end-kryptering finns på stora plattformar som t.ex. Apple iMessage, Facebook Messenger och WhatsApp, samt meddelandeplattformen Telegram.

15. Utan end-to-end-kryptering kan andra parter än avsändaren och de avsedda mottagarna se och läsa det ursprungliga meddelandet. Exempel på tillämpningar där end-to-end-kryptering normalt inte används är t.ex. e-posttjänster, där tjänsteleverantören kan läsa e-postmeddelanden som sparats i en personlig ”inkorg”, SMS och fax, där nätverksleverantören som tillhandahåller infrastrukturen mellan parterna också kan läsa innehållet i meddelandet när det passerar genom dess infrastruktur. Ett vykort som skickas via traditionell posthantering är ett icke-tekniskt exempel på hur vem som helst kan läsa meddelandet på dess väg från avsändaren till mottagaren.

16. ANØM använder XMPP (Extensible Messaging and Presence Protocol) för kommunikationen mellan deltagarna i ANØM. XMPP är erkänt av branschen och är ett offentligt tillgängligt ramverk som kan modifieras, anpassa och byggas ut efter behov.

17. Med ANØM kan deltagarna skicka end-to-end-krypterade meddelanden – bestående av text och bilagor som t.ex. bilder, videor, anteckningar och korta röstmeddelanden – till andra ANØM-användare.

18. Varje användare i ANØM identifieras med en unik identifierare (användar-ID), som tekniskt kallas för en Jabber Identifier (JID). Från början hade detta användar-ID formen av 6 alfanumeriska tecken (till exempel ”aab2c3”) och det genererades automatiskt från enhetens IMEI-nummer (International Mobile Equipment Identity number).

19. Enhetens IMEI-nummer kombinerades med en fast uppsättning tecken (en så kallad ”saltsträng”) för att skapa ett indatavärde. Indatavärdet genomgick en hashprocess i algoritmen MD5. De sista sex tecknen i det hashvärde som genererades var enhetens användar-ID och användarens lösenord var hela hashvärdet. Processen genomfördes automatiskt av ANØM-appen som använda detta användar-ID och lösenord för automatisk autentisering mot ANØM-servrarna.

20. Det är möjligt att beräkna användar-ID-t för ett visst IMEI eftersom MD5-processen, inklusive saltvärdet, är känd för AFP.

A.4 Portalen

21. Portalen var en webbplats som lanserades i januari 2021 av ANØM-operatören. Där kunde man hantera slutanvändares konton, enheter och abonnemang.

22. Åtkomst till portalen var generellt begränsad till återförsäljare av enheter och ANØM-administratörer, och den hade funktioner för att konfigurera nya enheter så att de skulle fungera i ANØM, ta bort en enhet eller genomföra en fjärrensning av en enhet. Åtkomsten till portalen skyddades av ett användarnamn och ett lösenord, och användaren var också tvungen att ansluta via en VPN-anslutning (Virtual Private Network) som bara var tillgänglig för dem som hade auktoriserats av ANØM-operatören.

23. På grund av förändringar i operativsystemet Android gick det från december 2020 inte längre att använda IMEI-numret till att automatiskt generera användar-ID. Formatet på användar-ID ändrades därför så att det genererades automatiskt i portalen. I den här processen består användar-ID av två slumpmässigt valda ord på engelska som satts samman. ”LITTLE” och ”FISH”

skulle t.ex. ge användar-ID:t ”LITTLEFISH”.

A.5 Enheter

24. Enheter som användes på ANØM bestod av smartphones som körde operativsystemet Android och som:

    a. Hade registrerats i en privat MDM-applikation (Mobile Device Management) som konfigurerades och kontrollerades av ANØM-administratörer. Med MDM-applikationen kunde administratörerna tillhandahålla eller begränsa vissa funktioner på enheterna.

    b. Hade den specialbyggda end-to-end-krypterade kommunikationsapplikationen (appen) installerad. Appen var bara tillgänglig på enheter som hade registrerats i MDM-applikationen.

25. Enheterna förbereddes innan de levererades till användaren. Förberedelserna innebar att den programvara som krävdes för att enheten skulle kunna komma åt och kommunicera via ANØM installerades och konfigurerades. Bilagorna B och C är två dokument som gavs ut av ANØM-administratörerna som riktlinjer för att förbereda enheterna. Förberedelserna omfattade:

    a. Installation av rätt version av operativsystemet, om det behövdes.

    b. Vid behov installation av ett aktivt SIM-kort (Subscriber Identity Module), som normalt hade köpts in från en av följande internationella leverantörer av mobilnätverk: Jersey Telecom (JT), Telefonica eller POD Group. SIM-korten behövde inte registreras i enhetsanvändarnas namn.

    c. Installation av MDM-applikationen och registrering av enheten i MDM.

    d. När registreringen i MDM var klar installerades ANØM-appen automatiskt på enheten.

    e. Om den installerade ANØM-appen var av en version som hade släppts senare än i januari 2021 behövde man använda portalen för att få ett automatiskt genererat användar-ID och lösenord som unikt kunde identifiera enheten i ANØM. Det krävdes inte för tidigare versioner av ANØM-appen, enligt förklaring i punkt 41.

    f. För de enheter som inte automatiskt kunde generera ett användar-ID och lösenord behövde ANØM-appen konfigureras med användar-ID och lösenord.

26. Slutanvändaren betalade en abonnemangsavgift till återförsäljaren för den period som han eller hon vill vara en aktiv användare av plattformen.

27. För de flesta ANØM-användare fanns det inga andra sätt att kommunicera på enheterna. Traditionella funktioner på mobiltelefoner, som t.ex. röst- eller videosamtal, SMS, appar för sociala medier, internetsurf och e-posttjänster, kunde inte användas på de tillhandahållna enheterna eftersom det förhindrades av MDM-inställningarna.

28. Den 8 juni 2021 hade bara 73 av ungefär 12 500 enheter förmågan att ringa i traditionell bemärkelse eller att surfa på internet via den installerade ToR-webbläsaren (The Onion Router). Det var tillåtet i MDM-inställningarna för en specifik grupp användare, så kallade COPE-användare (”Corporate Owned, Personally Enabled”).

29. Eftersom ANØM kördes på ett slutet nätverk, använde en privat app och krävde specifika

autentiseringsuppgifter gick det inte att oavsiktligt skicka ett meddelande via plattformen från en normal mobiltelefon.

30. Varje mobil enhet kan unikt identifieras genom dess IMEI-nummer. IMEI-numret är ett nummer med 15 siffror (14 siffror plus en kontrollsiffra) som ger information om enhetens märke, modell och serienummer. IMEI-numret är ofta tryckt på enheten.

31. De första 8 siffrorna i IMEI-numret kallas för TAC (Type Allocation Code) och identifierar enhetens märke (tillverkare) och modell. De efterföljande 6 siffrorna är enhetens serienummer, och den sista siffran är en kontrollsiffra som beräknas med Luhn-algoritmen.

32. IMEI-numret 358503082383242 består t.ex. av:

    a. TAC-numret 35850308, som identifierar IMEI-numret som tillhörande en Samsung Galaxy Note 8 och

    b. serienumret 238324 och

    c. kontrollsiffran 2.

33. Medan ANØM var i drift tillhandahölls enheter av olika märken och modeller. De vanligaste var Google Pixel, Samsung Galaxy och Xiaomi. Alla enheter körde en version av operativsystemet Android.

A.5 Nätverksanslutning till plattformen

34. Enligt beskrivningen i punkt 42.b.ii kan enheter tillhandahållas till slutanvändaren med ett internationellt SIM-kort som möjliggör internationell roaming över ett mobilnätverk i det land där enheten används. Slutanvändaren kan också köpa ett eget SIM-kort från en leverantör av telekommunikationstjänster.

35. Eller så kan enhetsanvändaren ansluta sig till ett tillgängligt WiFi-nätverk istället för att använda mobildata.

A.6 MDM-komponenten

36. För driften av ANØM användes två MDM-applikationer med tillhörande infrastruktur, MobileIron and FieldX. Båda MDM-applikationerna har liknande kärnfunktioner enligt beskrivningen nedan.

37. MDM-komponentens roll var att tillhandahålla och verkställa vissa enhetsfunktioner genom tillämpning av en MDM-policy som angavs av ANØM-administratörerna. Sådana funktioner kunde t.ex. vara att:

    a. Initiera en ”fjärrfabriksåterställning” av en enhet, vilket innebar att alla data raderades från enheten, inklusive appar.

    b. Verkställa en lösenordspolicy för enheten genom att se till att lösenordet uppfyllde vissa krav på komplexitet, t.ex. minsta längd och teckenuppsättningar.

    c. Förhindra att ”utvecklaralternativ” aktiverades, vilket hade kunnat göra det möjligt för en användare att aktivera USB-felsökning eller andra alternativ som kunde användas för att kringgå begränsningar för enheterna eller på andra sätt manipulera enheten.

    d. Upprätthålla en säker startinläsare som säkerställde att bara det operativsystem för mobila enheter som hade godkänts för plattformen fick köras, vilket därmed upprätthöll enhetens integritet och säkerhet.

e. Förhindra installation av ej betrodda eller ej godkända applikationer och därmed säkerställa att endast applikationer som var tillgängliga via MDM-komponenten för ANØM kunde installeras och köras på enheten.

f. För FieldX MDM: se till att ANØM-appen uppdaterades automatiskt.

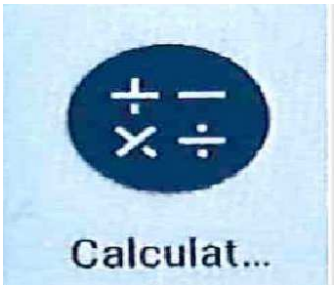
g. Rapportera information om enheten med jämna mellanrum, t.ex. enhetens unika IMEI-nummer, efterlevnad av MDM-policyn, enhetens startinläsare och version av operativsystemet samt enhetens status, t.ex. batterinivå och ledigt minnesutrymme.

38. MDM-komponenten använde funktioner som är en del av operativsystemet Android på enheten, kommunicerade med MDM-servrar för att rapportera enhetens status och hämtade policyer som skulle verkställas på enheten.

A.7 ANØM-applikationen

39. ANØM-applikationen (appen) finns på enheten men är dold i form av en fungerande kalkylatorapp. Varken appikonen eller kalkylatoretiketten avslöjar applikationens verkliga syfte. Om enheten undersöks av en ovetande användare finns det inget som visar att det finns en applikation för krypterade meddelanden på enheten.

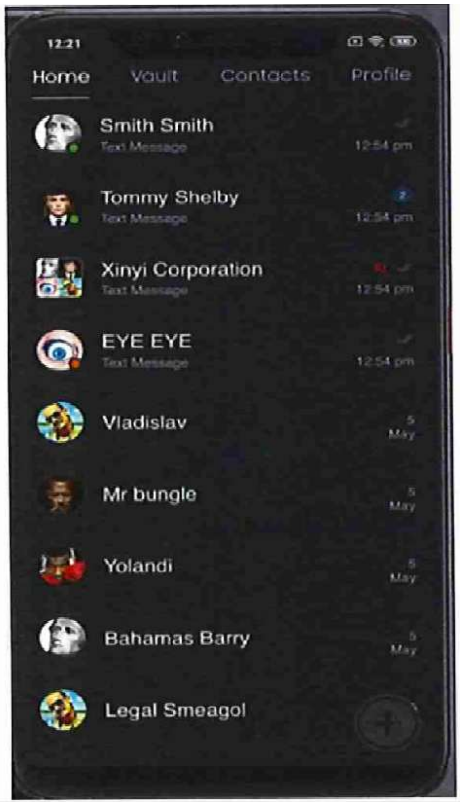
40. Här är ett exempel på appikonen som den såg ut på vissa enheter (ikonens utseende varierade beroende på version av operativsystemet):



41. När appen startas ser användaren ett gränssnitt som fortfarande ser ut som en kalkylator:

42. Kalkylatorn fungerar som förväntat, dvs. användaren kan mata in matematiska funktioner och det korrekta resultatet matas ut.

43. Men om användaren anger en hemlig PIN-kod och sedan håller ned lika-med-tecknet (=) visas den verkliga plattformsapplikationen:



44. Förutom PIN-koden för åtkomst till appen finns även en PIN-kod för nödlägen. Om den senare anges tillsammans med en nedtryckning av lika-med-tecknet raderas all information från appen.

45. PIN-koden för nödlägen kan t.ex. ges till en obehörig användare av enheten om ägaren tvingas eller frivilligt går med på att öppna appen. Appen öppnas som vanligt, men alla data raderas från appen. Ett exempel är om brottsbekämpande myndigheter tar enheten i beslag och kräver att få veta PIN-koden för åtkomst. Den behöriga användaren kan då istället uppge PIN-koden för nödlägen och därmed få det att se ut som att han eller hon samarbetar med utredningen, men i

själva verket raderas eventuellt bevismaterial.

A.7.1 ANØM-applikationsattribut

A.7.1.1 Identifierare för användare

46. Varje användare av plattformen identifieras med ett unikt användar-ID. Bara en enhet vid varje given tidpunkt kunde komma åt ANØM med ett visst användar-ID.
När användar-ID:t och lösenordet hade angetts i appen uppdaterade appen automatiskt lösenordet som var associerat med det användar-ID:t i ANØM. Det uppdaterade lösenordet sparades av appen för senare inloggningar, men det visades aldrig för och var inte känt av användaren som angav värdena. Försök att logga in på en annan enhet med tidigare lösenordet och användar-ID:t misslyckades, och lösenordet behövde återställas till ett känt värde för att det skulle lyckas.

A.7.1.2 Användarens visningsnamn

47. Enhetens användare kunde ange ett ”visningsnamn” (som också kallas smeknamn eller alias), som kunde ändras när användaren ville. Det förändrade inte deras användar-ID på plattformen. Det här liknar ”Från”-namnet som visas i e-postmeddelanden, som normalt skiljer sig från e-postadressen som ofta är användarnamnet.

A.7.1.3 Valvet

48. I valvet kan användaren på ett säkert sätt lagra anteckningar och bilder på enheten. Dessa data krypteras så att de bara kan kommas åt från enheten, och inga data i valvet skickas vidare om inte användare inkluderar dem som en bilaga till ett meddelande.

49. Anteckningar som sparas i valvet kan innehålla en rubrik samt brödtext eller en punktlista. Bilder som sparas i valvet eller som tas med enhetens kamera kan också infogas i anteckningar.

A.7.1.4 Meddelanden

50. En användare kan skicka ett end-to-end-krypterat meddelande till en annan ANØM-användare, förutsatt att de känner till mottagarens användar-ID.

51. En användare kan också skicka end-to-end-krypterade meddelanden till en grupp av ANØM-användare, och varje användare i den gruppen kan se de andra medlemmarna i gruppen. Gruppen kan ha en etikett som fungerar som ett namn på gruppen och som kan anges av gruppadministratören – normalt den som skapade gruppen – eller andra medlemmar som har fått administratörsbehörigheter för gruppen. Det här fungerar på ett liknande sätt som gruppchattar i andra meddelandeapplikationer som WhatsApp, Signal, Telegram och Facebook Messenger.

52. Ett meddelande, antingen till en enda användare eller till en grupp av användare, kan bestå av ett textmeddelande, en bild (t.ex. ett foto som togs med kameran på enheten), en video som spelats in med kameran på enheten, ett kort röstmeddelande (PTT – push-to-talk) eller en anteckning från enhetens valv.

53. Meddelanden kan vara på olika språk. För att kunna stödja olika språks teckenuppsättningar kan datorapplikationer använda Unicode som ett sätt att representera symboler och text från de flesta av världens skriftsystem. Unicode har ett unikt nummer för varje tecken, oavsett plattform, enhet, applikation eller språk. Det görs genom att tecken uttrycks som ett kodnummer och inte som glyfer. De arabiska tecknen ”ا ب و” skulle t.ex. representeras som ”\u0627\u0628\u0648” i Unicode. Så kallade ”emojis” kan också uttryckas som Unicode-värden. T.ex. är ”\u1F603” Unicode-värdet för emojin ”😃”. Sådana Unicode-värden måste konverteras tillbaka till de rätta tecknen för att de ska kunna läsas.

Applikationer kan tolka Unicode-värdet och visa tecknen istället för koden.

54. Det går att citera ett meddelande genom att välja det i en konversation och trycka på svara-knappen, eller vidarebefordra det till andra mottagare genom att välja det och trycka på dela-knappen. När det görs kan deltagarna i konversationen visuellt se att meddelandet har citerats eller vidarebefordrats eftersom det visas som ett citerat block i det skickade meddelandet.

55. Till skillnad från andra meddelandeapplikationer som t.ex. WhatsApp eller Telegram hade ANØM-appen inte några indikatorer för att ange om ett meddelande hade tagits emot eller lästs av mottagaren.

56. Möjlighet att ändra tonhöjd

    57. Avsändaren av ett ljudmeddelande kan justera tonhöjden på inspelningen innan den spelas in, antingen upp (alternativet ”Helium” i appen) eller ned (alternativet ”Jellyfish” i appen), vilket maskerar det verkliga ljudet i avsändarens ljudklipp för mottagaren. Avsändaren kan också välja att inte ändra tonhöjd.

A.7.1.5 Självförstörande meddelanden

58. Avsändaren av ett meddelande av någon av de typer som beskrivs ovan kan också ange en ”självförstörandetimer” för det meddelandet. Genom att ange en sådan tid tas meddelandet bort från alla enheter som har mottagit det när den inställda tidsperioden löper ut.

A.8 Data spelas in från plattformen

59. ANØM-appen hade en funktion som innebar att när ett meddelande skickades så skickade appen automatiskt en dold kopia av meddelandet till ett ghostanvändar-ID, ”bot”. Den här processen var inte synlig för den användare som skickade meddelandet, och användaren visste inte heller om att processen ägde rum.

60. Processen med den automatiska dolda kopian ledde till att en kopia av meddelandet krypterades och skickades till ghostanvändar-ID:t ”bot”. Datorer med en applikation som var kompatibel med plattformen tog emot de krypterade meddelanden som skickades till användar-ID:t ”bot”.

61. Processen för det var precis likadan som plattformens normala beteende när ett meddelande skickades, med undantag för att meddelanden som skickades till ghostanvändar-ID:t inte var synliga för de andra deltagarna i kommunikationen.

62. I avsnitt 1.5 finns ett diagram som visar meddelandeflödet och krypteringsprocessen för ett hypotetiskt meddelande som skickas från Alice till Bob, inklusive den dolda kopian och krypteringen för ghostanvändar-ID:t ”bot”.

63. A.8.1 Innehåll i meddelanden
64. Meddelanden som skickas med plattformen har oftast följande, eller en kombination av följande, attribut. De är synliga för både avsändare och mottagare:

    a. Självförstörelsetid – Anges av avsändaren när meddelandet skickas och definierar hur länge ett meddelande finns kvar innan det tas bort automatiskt från båda enheterna när tiden har löpt ut. Tiden syns på både avsändarens och mottagarnas enheter längst ned i varje meddelande. Den kan anges till 30 sekunder, 5 eller 30 minuter, 1 eller 12 timmar eller 1, 3 eller 7 dagar.

    b. Avsändare – användar-ID och visningsnamn för den avsändande enheten.

    c. Mottagare – Mottagarna av ett meddelande kan identifieras genom att visa deltagarna i

meddelandetråden i fråga. Liksom i andra populära chattapplikationer som t.ex. WhatsApp, Telegram och Facebook Messenger visas de som separata poster i en meddelandelista.

d. Innehåll – Meddelandets innehåll som kan bestå av text eller en bilaga som ljud, bild, video eller anteckning.

e. Tid – Tid och datum i GMT (Greenwich Mean Time) enligt den avsändande enheten när ett meddelande skickades. Det visas på enheten i den inställda tidszonen. Ett meddelande som skickades den 10 juni 2020 kl. 11. 00 Perth-tid skulle t.ex. ha datum och tid kl. 03. 00 den 10 juni 2020 GMT. En enhet i Sydney skulle visa den tiden som kl. 13. 00 den 10 juni 2020. Enheter med ett aktivt SIM-kort synkroniserade sin tid via NTP (Network Time Protocol) till det operatörsnätverk som den var ansluten till.

    i. Se avsnitt 8.6.1 för information om tidszonsavvikelser.

A.8.2 Metadata för meddelanden

65. Meddelanden som skickades via ANØM innehöll ytterligare metadata som inte var synliga varken för avsändaren eller mottagaren av ett meddelande. Vissa av fälten inkluderades för att vara till hjälp för brottsbekämpande myndigheter. På grund av förändringar och tillägg skickades inte alla metadatafälten nedan med varje meddelande:

    a. Ett unikt meddelande-ID – Ett UUID (Universally Unique Identifier) som genererades automatiskt av den avsändande enhetens applikation då ett meddelande skickades. Det visades varken för avsändaren eller mottagarna av ett meddelande. Det här är en komponent i XMPP-ramverket.

    b. IMEI – På enheter som körde operativsystemet Android i version 9 eller lägre inkluderades IMEI-numret som metadata med varje meddelande för användning av brottsbekämpande myndigheter.

    c. MCC/MNC – Enheter med ett aktivt SIM-kort som var registrerade på ett mobilt kommunikationsnätverk skickade den MCC-kod (Mobile Country Code) och den MNC-kod (Mobile Network Code) som enheten för närvarande var uppkopplad mot. De siffrorna skickades med som metadata med meddelandet för användning av brottsbekämpande myndigheter.

    d. Platsinformation – Efter en uppdatering av appen i april 2020 försökte appen ta fram platsinformation via Androids API Location Manager. Om det gick att fastställa en plats inkluderades latitud, longitud, noggrannhet och tidpunkten för platsbestämningen som metadata med meddelandet för användning av brottsbekämpande myndigheter. Ibland kunde appen inte hitta en fullständig och korrekt GPS-plats. När det hände inleddes den hämtade GPS-punkten ofta med siffrorna 39,0 och pekade på en plats utanför Fijis kust i södra Stilla Havet.

    e. Tonhöjdsjustering för ljud – Om meddelandet innehöll en ljudbilaga inkluderades metadata som angav värdet för tonhöjdsjusteringen för användning av brottsbekämpande myndigheter.

    f. Citerade eller vidarebefordrade meddelanden – Om ett meddelande innehöll ett citat eller var ett vidarebefordrat meddelande innehöll det nya innehållet i meddelandet det citerade eller vidarebefordrade innehållet, som också kunde innehålla information som användar-ID för den ursprungliga avsändaren och tidpunkten för det ursprungliga meddelandet. Det här var en funktion i ANØM-appen. Andra meddelandeapplikationer

som t.ex. WhatsApp, Signal, Telegram och Facebook Messenger har en liknande funktion för att citera och vidarebefordra meddelanden.

A.9 Autentisering och integritet

66. Eftersom ANØM-appen uppdaterade lösenordet vid den första inloggningen förhindrade den enheter från att autentisera och skicka meddelanden i ett annat ANØM-användar-ID:s namn. Mer information kommer i en framtida bilaga.

67. Fram tills förändringen av formatet för användar-ID i december 2020 var användar-ID direkt relaterat till enhetens IMEI-nummer, vilket ytterligare begränsade möjligheterna att skicka ANØM-meddelanden.

68. Om en enhet ”fabriksåterställdes”, antingen via MDM eller direkt på enheten, togs alla data och applikationer – även MDM-appen och plattformsappen – bort från enheten.

69. Om PIN-koden för nödlägen angavs togs alla data, inklusive sparade inloggningsuppgifter, bort från appen. Därmed kunde användaren inte komma åt eller kommunicera via ANØM.

70. Om någon av dessa processer genomfördes behövde användar-ID och lösenordet återställas innan enheten kunde användas för att komma åt ANØM igen. Vid en fabriksåterställning behövde enheten ometableras.

ORDLISTA

- **AES-kryptering**: Symmetrisk kryptering (med enkel nyckel) som användes för den andra delen av återkrypteringen av inhämtade data.
- **ANØM**: En kommunikationsplattform med end-to-end-kryptering som använde särskilda mobiltelefonenheter med en anpassad, installerad meddelandeapplikation för att kommunicera inom ett slutet nätverk.
- **API (Application Programming Interface)**: Ett programvarugränssnitt som oftast används med dator-till-dator-interaktion där en klientdator initierar en förfrågan som besvaras av serverdatorn som kör API:t, vilken normalt returnerar data till den klientdator som skickade förfrågan.
- **AWS GovCloud**: Amazon Web Services molninfrastruktur där webbapplikationen Hola iBot och data relaterade till Operation Trojan Shield lagrades.
- **Startinläsare**: Den första programvara som körs på en mobiltelefon när enheten slås på eller startas om. Den initialiserar maskinvaran och läser in operativsystemet, t.ex. Android.
- **Ärenden**: Kallas också syndikat. Det här är den centrala komponenten för relationer i databasen iBot_dec.
- **Skillnadsdump**: Nya eller ändrade data mellan två MySQL-databasdumpar. Det är metoden för hur det tredje landet tog fram nytt innehåll ur hela databasen då det skickade nya datapaket.
- **Elastic Compute Cloud (EC2)**: Datorresurser som ägs av AWS och som kan hyras för att köra datorprogram.
- **End-to-end-kryptering**: Kryptering där data krypteras mellan två ändpunkter och där endast de ändpunkterna har förmåga att avkryptera data. Data kan inte avkrypteras av de servrar och nätverk som data passerar mellan de två ändpunkterna.
- **XMPP (Extensible Messaging and Presence Protocol)**: XMPP är ett öppet standardprotokoll för snabbmeddelanden som möjliggör chattar mellan flera parter. Det har stöd för multimedia som röst, bilder och video. Vem som helst kan köra en egen XMPP-server och nätverk och bygga vidare på det befintliga ramverket.
- **Ghostanvändar-ID (”bot”)**: Det användar-ID till vilket ANØM-applikationen på mobila enheter skickade en dold kopia av alla meddelanden som skickades från den enheten.
- **GPG (GnuPG)**: Möjliggör kryptering av data och signering av kommunikation.
- **Google Compute Engine**: En tjänst från Google Cloud som gör det möjligt att skapa och köra virtuella datorer i Google Cloud.
- **Hash (MD5, SHA-2)**: En hashfunktion är en matematisk process där indata, ”meddelandet”, bearbetas till ett ”sammandrag av meddelandet” eller ett hashvärde med fast längd. Det anges ofta som hexadecimala tecken med siffrorna 0 till 9 och bokstäverna A till F. Hashfunktioner används ofta för dataverifiering genom att identifiera om data har förändrats, eftersom det är mycket osannolikt att två olika ”indatameddelanden” resulterar i samma hashvärde.
- **Hola iBot**: Den anpassade webbapplikation som skapades och drevs av FBI i San Diego och som fungerade som granskningsplattform för alla data som togs emot från plattformen ANØM.

- **iBot_dec**: Databasen som skickade data till granskningsplattformen Hola iBot. Innehåller data som samlades in på plattformen ANØM och skickar den för granskning.
- **iBot_enc**: Den tillfälliga databas där nya datapaket förvarades när nya data togs emot från servern i det tredje landet.
- **Servern Ingestion-1 (I1)**: Den AWS GovCloud EC2 som körde inmatningsprocessen (avsnitt 9), sparade filer som bifogats till meddelanden och skickade data till databasen iBot_dec.
- **IMEI (International Model Equipment Identifier)**: Ett 15-siffrigt nummer som tilldelas en mobil enhet och som kan användas som identifierare. Det består av ett 8-siffrigt TAC-nummer (Type Allocation Code) som visar enhetens märke och modell, ett 6-siffrigt serienummer och en kontrollsiffra (sista siffran) som beräknas med Luhn-algoritmen.
- **Platsinformation**: Information som identifierar en plats (som kan vara en region eller ett område). Den består normalt av värden för latitud och longitud samt en tidsstämpel i UTC för den tid då platsen fastställdes. Platsen kan fastställas med GNSS (Global Navigation Satellite Systems) som t.ex. GPS eller GLONASS, eller fastställas utifrån information om närliggande mobilmaster och WiFi-åtkomstpunkter.
- **MCC (Mobile Country Code)**: MCC-koden identifierar unikt ursprungslandet för mobilabonnenten och är de tre första siffrorna i IMSI-numret (International Mobile Subscriber Identity) som lagras på SIM-kortet. Australien har t.ex. MCC-värdet 505.
- **MDM (Mobile Device Management)**: En programvaruapplikation som består av en mobil enhetskomponent och en serverkomponent som ofta används för att tillämpa vissa funktioner på enheter, så kallade policyer, för att förbättra enheternas integritet, säkerhet och användarvänlighet. MDM-applikationer har ofta också möjligheten att tömma enheter på information på distans.
- **MNC (Mobile Network Code)**: MNC-koden består av två eller tre siffror som identifierar mobilabonnentens mobilnätverk. Det är de två eller tre siffrorna som följer på MCC-koden som tillsammans utgör IMSI-numret (International Mobile Subscriber Identity) som lagras på SIM-kortet. Följande exempel kommer från australiska mobilnätoperatörer (inte ett heltäckande exempel): Telstra har 01, Optus har 02och Vodafone har 03.
- **MySQL-dump**: En logisk säkerhetskopia av alla tabeller, inklusive innehåll, i en MySQL-databas.
- **Nytt datapaket**: Ett paket med nya data hämtade från ANØM-plattformen som skickades av det tredje landet till I1-servern.
- **Portal**: En webbplats som nås via internet med en VPN-anslutning (Virtual Private Network). Man loggar in med ett giltigt användarnamn och lösenord från ANØM-administratörerna och kan då hantera ANØM-slutanvändares enheter, konton och användar-ID:n.
- **Proxy**: En server som fungerar som ett relä för all nätverkstrafik mellan två datorer eller servrar.
- **Kryptering med offentlig nyckel**: Ett system för kryptering och avkryptering där ett par matematiskt relaterade nycklar används för att kryptera och avkryptera innehåll. Den ”offentliga” nyckeln kan användas för att kryptera innehåll som bara den ”privata” nyckeln kan avkryptera, och tvärtom. Samma nyckel kan inte användas för att avkryptera innehåll som krypterades med den.
- **RAM**: Tillfällig lagring i en dator. T.ex. lagrades alla tillfälliga datastrukturer i RAM-minne

inför inmatningen.

- **RSA-kryptering:** En typ av PKI-kryptering som delvis användes för återkryptering av inhämtade data.
- **SIM (Subscriber Identity Module)**: SIM-kortet är ett fysiskt integrerat kretskort som lagrar IMSI-numret (International Mobile Subscriber Identity) och dess relaterade autentiseringsnyckel, som används för att unikt identifiera och autentisera en mobilabonnent (slutanvändare) i ett mobilt nätverk. SIM-kortet har också ett unikt serienummer som kallas ICCID (Integrated Circuit Card Identifier) och som kan vara tryckt på SIM-kortet.
- **TLS (Transport Layer Security)**: En implementering av kryptering med offentlig nyckel som ofta används för att säkra information som skickas till och från webbplatser, t.ex. banker, e-post och sökmotorer på internet. Man kan se att det används genom att det visas en bild av ett låst hänglås i webbläsarens adressfält. TLS kan också användas för att göra annan kommunikation säker, t.ex. snabbmeddelandeapplikationer och VoIP-kommunikation (Voice over Internet Protocol).
- **Unicode**: Unicode är en metod för att representera symboler och text från de flesta av världens skriftsystem. Det görs genom att tecken uttrycks som ett nummer och inte som glyfer. ”Emojis” är en vanlig typ av glyf som skulle uttryckas med Unicode-värdet i t.ex. meddelandeapplikationer men som visas för avsändaren och mottagaren som en glyf.
- **USB-felsökning**: Möjligheten att ansluta en dator till en mobil enhet via en USB-kabel (Universal Serial Bus) och interagera med operativsystemet i den mobila enheten. Det kan användas till att lägga till eller ta bort data från enheten, läsa loggar eller installera och ta bort applikationer. Det kan också användas till att byta operativsystem på en mobil enhet eller installera processer som körs med höjda behörigheter – så kallad ”rooting”.
- **Användar-ID (JID)**: Ett användarnamn som unikt identifierade en användare på ANØM-plattformen. Från början bestod det av sex tecken hämtade från siffrorna 0 till 9 och bokstäverna A till F, och senare blev det två slumpmässigt valda engelska ord som kombinerades.
- **VPN (Virtual Private Network)**: En nätverksapplikation som används för att kryptera data som skickas över en ej betrodd nätverksanslutning, vanligtvis internet. VPN användes traditionellt till att via en internetanslutning ”utöka” ett privat nätverk, dvs. ett nätverk som inte är åtkomligt om man inte är direkt uppkopplad mot det, exempelvis ett företagsnätverk. På så sätt kan en fjärransluten enhet komma åt webbplatser, filer, data och tjänster som inte är tillgängliga utanför det privata nätverket. VPN kan även användas för att dölja en användares identitet eller deras aktivitet på internet från användarens internetleverantör.
- **XMPP**: *Se Extensible Messaging and Presence Protocol (XMPP)*

A605.834-2021

IT-avdelningen

Anøm

Beskrivning av information i Anom-data

Rapport
Version 2.0
2022-02-28

Utgivare
Polismyndigheten
Tfn 114 14
E-post kansli.registrator@polisen.se
www.polisen.se

Produktion Polismyndigheten, 2022-02-28

Diarienr. A605.844/2021

A605.834-2021

Tryck Polisens tryckeri

Sammanfattning

Polismyndighetens IT-avdelning har på uppdrag av Polisens nationella operativa avdelning (NOA) utvecklat och applicerat en metod för hantering av det material som inkommit i operation Trojan Shield som berör dekrypterad information från kommunikationstjänsten Anom.

Det här dokumentet beskriver *innehållet,* bestående av meddelanden, användarkonton och metadata, i den dekrypterade informationen.

För beskrivning av Polisens *hantering* av dekrypterad information från Anom hänvisas till dokumentet ”*A605.844/2021 Beskrivning av Polisens hantering av Anom-data*”

Revisionshistorik

Datum	Version	Kommentar	Avsändare
2021-09-21	1.0	Initial version	IT-avdelningen
2022-02-28	2.0	Större bearbetning med förtydliganden och tillägg av flertalet kapitel.	IT-avdelningen

Innehållsförteckning

1 Inledning

1.1 Bakgrund

Sammanlagt har 16 länder ingått i insatsen med namnet Trojan Shield/OTF Greenlight. I Europa har arbetet letts av Sverige och Nederländerna i samarbete med Europol.

Den krypterade plattformen Anom, har använts av kriminella för att kunna planera, koordinera och utföra brott. Plattformen skapades och administrerades i det dolda av FBI. I takt med att liknande tjänster som ”*Encrochat*” och ”*Sky ECC*” upphörde övergick allt fler kriminella aktörer till att kommunicera på denna plattform.

Enligt FBI har över 27 miljoner meddelanden skickats via plattformen av över 200 kriminella nätverk mellan oktober 2019 och juni 2021 [1].

Efter att plattformen avvecklades i juni 2021 har Polismyndigheten av FBI försetts med exporter av meddelanden och annan information från plattformen i enlighet med det ömsesidiga juridiska biståndsavtalet (MLAT) mellan USA och EU.

1.2 Syfte

Dokumentet syftar till att beskriva innehållet av det material som mottagits i MLAT. Den första delen (avsnitt 2) beskriver vad rubrikerna och tabellinnehållet betyder. Den andra delen (avsnitt 3) utgörs av observationer som gjorts vid hantering av materialet, som är relevanta för att förstå det på ett korrekt sätt.

1.3 Hänvisning till OTS Technical Details

I detta dokument finns flertalet hänvisningar till det tekniska dokument som är framtaget av FBI gällande Operationen Trojan Shield (OTS) [2]. Det tekniska dokumentet finns i en engelsk och en svensk version. Hänvisningar till respektive kapitel och eventuellt avsnitt är densamma i både det svenska och det engelska dokumentet. Dessa hänvisningar betecknas med kursiv stil *OTS kap. <kapitel>.<avsnitt> <svensk rubrik>*. Exempelvis: *OTS kap. 8.1 Ärenden/syndikat.*

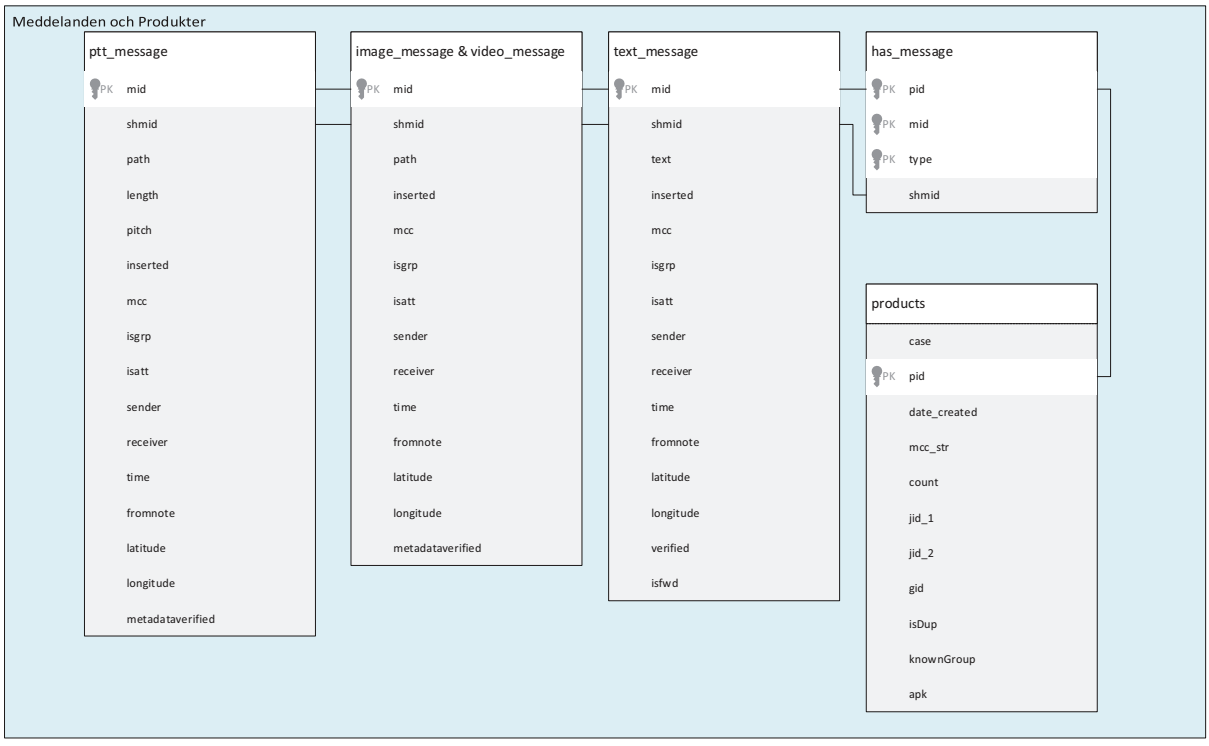
2 Innehåll i MLAT-exporter

2.1 Databasstruktur

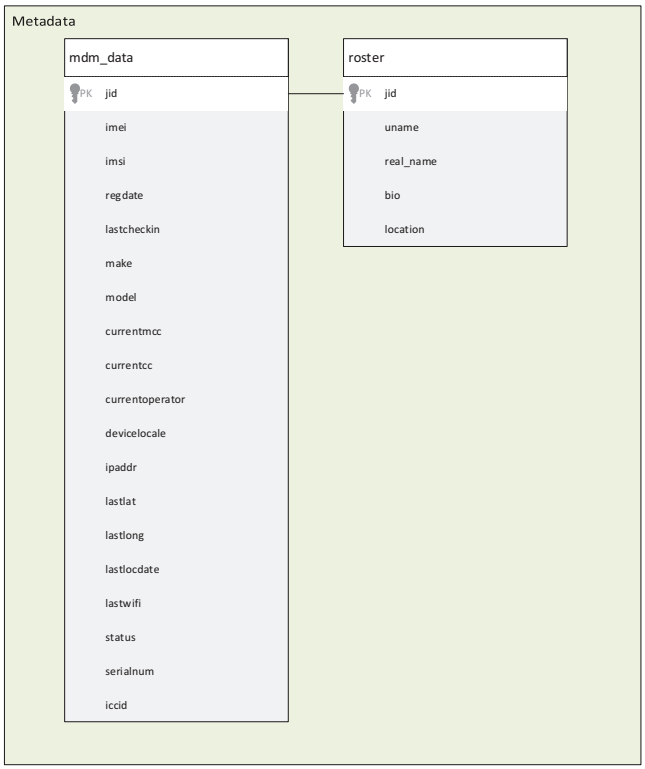
Varje MLAT-export innehåller instruktioner för att bygga upp en SQL-databas innehållandes följande tabeller:

```
has_message
ptt_messages
image_messages
video_messages
text_messages
products
mdm_data
roster
```

Nedan är en visualisering av databas-strukturen samt dess relationer



Figur 1 Databasstruktur meddelanden



Figur 2 Databasstruktur metadata

2.2 Databasinformation

Nedan följer en kort beskrivning av tabeller och dess innehåll.

2.2.1 Has_message

Tabellen beskriver relationerna mellan produkter och meddelanden och innehåller följande fält:

Fält	Betydelse/tolkning
pid	Produkt-ID för aktuell mid
mid	Meddelande-ID
type	Typ av meddelande. Kan vara 1:text, 2:bild, 3:push-to-talk/ljud, 4:video.
shmid	Meddelande UUID

2.2.2 Ptt_message

Tabellen innehåller samtliga ljudmeddelanden genererade av plattformens push-to-talk (PTT)-funktion. Dessa meddelanden kunde även förvrängas med hjälp av en tonhöjdsjustering.
Tabellen innehåller följande fält:

Fält	Betydelse/tolkning
mid	Meddelande-ID, återfinns även i has_message.
shmid	Meddelande-UUID, återfinns även i has_message.
path	Sökväg till aktuell media-fil.
length	Tomt fält.
pitch	Ursprunglig tonhöjd på meddelandet.
inserted	Tid och datum då meddelandet lästes in Ingestion-1, *OTS kap. 1.4.3 Ingestion-1.*
mcc	Mobile Country Code för meddelandet.
isgrp	Anger om meddelandet är en del av en gruppkonversation.
isatt	Anger om meddelandet är en bilaga till ett annat meddelande.
sender	Sändande JID på meddelandet.
reciever	Mottagande JID och/eller grupp (gid).
time	Tid då meddelandet skickades.
latitude	Latitud för den enhet som skickat meddelandet.
longitude	Longitud för den enhet som skickat meddelandet.
metadataverified	Tomt fält.

2.2.3 Image_message & video_message

Tabellen innehåller samtliga meddelanden där bilder eller videoklipp ingick.
Tabellen innehåller följande fält:

Fält	Betydelse/tolkning
mid	Meddelande-ID, återfinns även i has_message.
shmid	Meddelande-UUID, återfinns även i has_message.
path	Sökväg till aktuell media-fil.
inserted	Tid och datum då meddelandet lästes in Ingestion-1, *OTS kap. 1.4.3 Ingestion-1.*
mcc	Mobile Country Code för meddelandet.
isgrp	Anger om meddelandet är en del av en gruppkonversation.
isatt	Anger om meddelandet är en bilaga till ett annat meddelande.
sender	Sändande JID på meddelandet.
reciever	Mottagande JID och/eller grupp (gid).
time	Tid då meddelandet skickades.
fromnote	Anger om meddelandet är skickat från enhetens ”valv”.
latitude	Latitud för den enhet som skickat meddelandet.
longitude	Longitud för den enhet som skickat meddelandet.
metadataverified	Tomt fält.

2.2.4 Text_message

Tabellen innehåller samtliga meddelanden innehållandes enbart text.
Tabellen innehåller följande fält:

Fält	Betydelse/tolkning
mid	Meddelande-ID, återfinns även i has_message.
shmid	Meddelande-UUID, återfinns även i has_message.
text	Textinnehåll i meddelande. Textinnehållet kan anta olika format och beskrivs närmre under 3.1 textformat.
inserted	Tid och datum då meddelandet lästes in Ingestion-1, *OTS kap. 1.4.3 Ingestion-1.*
mcc	Mobile Country Code för meddelandet.
isgrp	Anger om meddelandet är en del av en gruppkonversation.
isatt	Anger om meddelandet är en bilaga till ett annat meddelande.
sender	Sändande JID på meddelandet.
reciever	Mottagande JID och/eller grupp (gid).
time	Tid då meddelandet skickades.
latitude	Latitud för den enhet som skickat meddelandet.
longitude	Longitud för den enhet som skickat meddelandet.
verified	Tomt fält.
isfwd	Anger om meddelandet är ett vidarebefordrat meddelande.

2.2.5 Product

Tabellen innehåller information om de trådar/produkter som genererats i exporter.
Tabellen innehåller följande fält:

Fält	Betydelse/tolkning
case_id	Det case/syndikat aktuell produkt tillhör. Ytterligare information om syndikat återfinns i OTS kap. 1.4.3 Ingestion.
pid	Produkt-ID, återfinns även i has_message.
date_created	Datum och tid då produkten skapats.
mcc_str	Mobile Country Code för samtliga meddelanden som skickats i produkten.
jid_str	Samtliga JID som skickat eller tagit emot meddelanden i produkten.
count	Antalet meddelanden i produkten.
jid_1	Ena parten vid tvåpartskommunikation, tomt vid gruppkonversation.
jid_2	Andra parten vid tvåpartskommunikation, tomt vid gruppkonversation.
gid	Grupp-ID vid flerpartskommunikation, tomt vid tvåpartskommunikation.
isDup	Tomt fält.
knownGroup	Tomt fält.
apk	Grupp-ID

2.2.6 MDM_Data

Tabellen innehåller information om Anom-enheter hämtat från plattformens Mobile Device Management-verktyg. Tabellen innehåller följande fält:

Fält	Betydelse/tolkning
jid	Aktuellt JID, återfinns tabellen Roster.
imei	Senast kända International Mobile Equipment Identity för enheten.
imsi	Senast kända International Mobile Subscriber Identity för SIM-kortet.
regdate	Datum då enheten registrerades i MDM-plattformen.
lastcheckin	Senast enheten syntes av MDM-plattformen.
make	Märke på enheten.
model	Modell på enheten.
currentmcc	Senast kända Mobile Country Code.
currentcc	Senast kända Country Code.
currentoperator	Senast kända teleoperatör.
currentphone	Senast kända telefonnummer.
devicelocale	Senast kända språk- och regionsinställningar på enheten.
ipaddr	Senast kända IP-address.
lastlat	Senast kända latitud.
lastlong	Senast kända longitud.
lastlocdate	Tid och datum för senast kända position.
lastwifi	Senast kända Wifi enheten kopplats till.
status	Status enheten förmedlade till MDM vid senaste incheckning.
serialnum	Serienummer på enheten.
Iccid	Integrated circuit card identifier på SIM-kortet.

2.2.6.1 Kompletterande MDM-information

Den 2021-11-16 delgavs kompletterande information om Anom-enheter. Tabellen innehåller följande fält:

Fält	Betydelse/tolkning
JID	Aktuellt JID, återfinns tabellen Roster.
IMEI	Samtliga kända International Mobile Equipment Identity för enheten.
ICCID	Samtliga kända Integrated circuit card identifier på SIM-kort.
Last Known Latitude	Senast kända latitud för enheten
Last Known Longi-tude	Senast kända longitud för enheten
Last Location Re-ported Time	Tid och datum för senast kända position.
Serial Number	Serienummer på enheten
Network Carrier	Senast kända teleoperatör
IMSI	Samtliga kända International Mobile Subscriber Identity för SIM-kort.
Model	Modell på enheten.
Last Seen	Senast enheten syntes av MDM-plattformen.

2.2.7 Roster

Tabellen innehåller känd information om brukaren av en JID. Tabellen innehåller följande fält:

Fält	Betydelse/tolkning
jid	Aktuellt JID, återfinns i tabellen MDM_Data
uname	Senast kända alias för aktuell JID
real_name	Det namn en användare av Hola iBot senast registrerat för aktuell JID
bio	Den beskrivning en användare av Hola iBot senast registrerat för aktuell JID
location	Den plats en användare av Hola iBot senast registrerat för aktuell JID

Användare av Hola iBot var polisanställda som ingick i operationen Trojan Shield som manuellt matade in denna information, vilket beskrivs ytterligare i *OTS kap 10.7 Förteckningssidan.*

3 Relevanta observationer av MLAT-materialet

Vid hanteringen av MLAT-materialet har följande observationer kunnat göras som är relevanta för en korrekt förståelse av materialet.

3.1 Produkter

Under Operation Trojan Shield skapades nya datapaket varje måndag, onsdag och fredag, *OTS kap. 2. Skapande av nya datapaket*. Samtliga konversationer mellan två individer eller i en grupp delades in i produkter, även kallat trådar eller chattslingor. Dessa förseddes med både case_id och pid. En produkt från syndikat 12 med pid 34567 presenteras som 12_34567. Dessa produkter innehåller samtliga meddelanden skickade i konversationen sedan senaste exporttillfället och löper således mellan två till tre dagar.

3.2 Textformat

Meddelanden som skickas via Anom kan antingen återfinnas som ren text, eller som något av de format som presenteras i avsnittet. Dessa är samtliga skrivna som JavaScript Object Notation (JSON).

Text i JSON innehåller normalt inga radbrytningar. Nedan exempel har radbrutits för ökad läsbarhet.

Varje kategori av meddelande finns i två versioner beroende på vilken tidsperiod meddelandet har blivit inläst till Anom-plattformen.

3.2.1 Vidarebefordrade meddelanden

När en användare vidarebefordrar ett meddelande från en konversation till en annan användare presenteras detta som en vidarebefordran (engelska: forward). Meddelanden som vidarebefordras kan presenteras på två sätt.

Vidarebefordringar inlästa till och med 2020-09-09 innehåller enbart text och presenteras som följande exempel:

```
forward_prefix
{
 "forward_message_time":     1633354850,
 "forward_message_text":     "hej",
 "forward_mes-               "abc123"
 sage_user_jid":
}
```

Värdetabell:

Fält	Betydelse/tolkning
forwarded_message_time	Tidsstämpel i Unix Time.
forward_message_text	Vidarebefordrat innehåll.
forward_message_user_jid	Den JID som meddelandet vidarebefordrats från.

Vidarebefordringar inlästa från och med 2020-09-11 möjliggör övriga typer av innehåll och presenteras som följande exempel:

```
forward_prefix
{
 "forward_message_time":     1633354850,
 "forward_mes-               "abc123",
 sage_user_jid":
 "forward_message_body":     "hej",
 "forward_message_type":     "TEXT”,
 "forward_message_uuid":     "123e4567-e89b-12d3-a456426614174000"
}
```

Värdetabell:

Fält	Betydelse/tolkning
forwarded_message_time	Tidsstämpel i Unix Time.
forward_message_user_jid	Den JID som meddelandet vidarebefordrats från.
forward_message_body	Den text eller kontaktinformation som vidarebefordrats. Om forward_message_type är IMAGE, VIDEO, PTT eller NOTE finns inte detta fält i meddelandet.
forward_message_type	Anger vilken sorts meddelande som vidarebefordrats. Fältet kan anta följande värden: TEXT, IMAGE, VIDEO, PTT, CONTACT och NOTE och avgör om det vidarebefordrade meddelandet är text, bild, video, ljud, kontaktinformation eller en anteckning.
forward_message_uuid	UUID på vidarebefordrat meddelande. Detta UUID är inte detsamma som meddelandets shmid.

3.2.2 Svar på meddelanden

När en användare svarar på ett specifikt meddelande i befintlig konversation representeras detta som ett citat (engelska: quote). Citat i konversationer kan presenteras på två sätt.

Meddelanden inlästa till och med 2020-12-21 (med ett fåtal undantag) presenteras som följande exempel:

```
quote_prefix
{
 "quote_message_time":       1633354850,
 "quote_message_text":       "Hur mår du?",
 "quoted_text":              "Jag mår bra",
 "quote_message_user_jid":   "abc123",
 "message_uid":              "123e4567-e89b-12d3-a456-426614174000"
}
```

Värdetabell:

Fält	Betydelse/tolkning
quote_message_time	Tidsstämpel i Unix Time.
quote_message_text	Det meddelande som har besvarats.
quoted_text	Det svar som getts.
quote_message_user_jid	Den JID som skickat det meddelande som har besvarats.
message_uid	UUID på det meddelande som besvarats. Detta UUID är inte detsamma som meddelandets shmid.

Meddelanden inlästa från och med 2020-12-25 (med vissa undantag) innehåller ytterligare metadata och innehåller förutom ovan även följande fält

```
quote_prefix
{
 "quote_message_time":       1633354850,
 ⋮
 "isQuotedMessageDeleted":   true,
 "isEdited":                 false,
}
```

Värdetabell:

Fält	Betydelse/tolkning
quote_message_time	Tidsstämpel i Unix Time.
isQuotedMessageDeleted	Anger om det besvarade meddelandet har raderats. Kan anta värdet true (sant) eller false (falskt).
isEdited	True/False. Anger om det besvarade meddelandet har redigerats.

3.2.3 Valvbilagor

När en användare skickar med en bilaga från det så kallade valvet presenteras det som en valvbilaga (engelska: vault attachment). Bilagor kan vara anteckningar och bilder, *OTS A.7.1.3 Valvet.* Valvbilagor kan presenteras på två vis.

Valvbilagor skickade till och med 2020-12-23 presenteras som följande exempel:

```
{
 "mIsSelected":              true,
 "passwordChecked":          false,
 "archived":                 true,
 "attachmentsList":          [],
 "attachmentsListOld":       [],
 "checklist":                false,
 "content":                  "",
 "creation":,
 "lastModification":,
 "locked":                   false,
 "reminderFired":            false,
 "title":                    "",
 "trashed":                  false
}
```

Värdetabell:

Fält	Betydelse/tolkning
mIsSelected	True/False, innebörd i dagsläget okänd.
passwordChecked	True/False, innebörd i dagsläget okänd.
archived	True/False, innebörd i dagsläget okänd.
attachmentsList	Detta fält innehåller i förekommande fall en lista med bilagor skickade i meddelandet.
attachmentsListOld	Detta fält är tomt i samtliga meddelanden.
checklist	Anger om innehållet är en checklista.
content	Detta fält innehåller i förekommande fall textinnehåll.
creation	Tid i Unix time som bilagan skapades.
lastModification	Tid i Unix time som bilagan senast ändrades.
locked	True/False, innebörd i dagsläget okänd.
reminderFired	True/False, innebörd i dagsläget okänd.
title	Bilagans titel.
trashed	True/False, innebörd i dagsläget okänd.

Meddelanden inlästa från och med 2020-12-23 presenteras som följande exempel.

```
{
 "mIsFromVault":              true,
⋮
}
```

Värdetabell:

Fält	Betydelse/tolkning
mIsFromVault	True/False, innebörd i dagsläget okänd.

Övriga fält som ovan.

3.3 Tidsförskjutning

3.3.1 Tidszonsdifferens

I källmaterialet för MLAT-exporter är samtliga tidsstämplar angivna som tidsformatet UTC. På grund av en misskonfiguration i en av servrarna som extraherat Anom-data har tidszonen för vissa meddelanden felaktigt tolkats som UTC fast den i själva verket varit en annan tidszon. FBI har identifierat olika tidsfönster som gäller för meddelanden *OTS kap. 8.6.1 Fel i meddelandens tidszon*. Meddelanden som är inlästa i respektive fönster är angivna som UTC men skall konverteras enligt nedan:

- Tidsram 1

  Meddelanden inlästa mellan 1 oktober 2019 och 27 oktober 2019: UTC -3

- Tidsram 2

  Meddelanden inlästa mellan 27 oktober 2019 och 29 mars 2020: UTC -2

- Tidsram 3

  Meddelanden inlästa mellan 29 mars 2020 och 18 september 2020: UTC -3

- Tidsram 4

  Meddelanden inlästa efter 18 september 2020: UTC

3.3.1.1 Exempel korrigering av tidszonsdifferens

Följande fyra exempelmeddelanden är inlästa 2020-08-28 och 2020-08-31 vilket framgår i kolumn MESSAGE_INSERTED. Dessa meddelanden faller således inom tidsram 3 (29 mars 2020 – 18 september 2020) och skall därför tolkas som UTC -3. I källmaterialet visas följande tidsstämplar:

	A	B	C	D	S
1	MESSAGE_TIME	MESSAGE_SENDER	MESSAGE_DECODED	MESSAGE_RECEIVER	MESSAGE_INSERTED
2	2020-08-27 17:48:46	Exempel1	Hej	exempel2	2020-08-28 00:11:09
3	2020-08-27 17:50:01	Exempel2	Hej på dig	Exempel1	2020-08-31 00:11:10
4	2020-08-27 17:50:15	Exempel1	Hur går det?	Exempel2	2020-08-31 00:11:10
5	2020-08-27 17:51:04	exempel2	Det går bra tack.	Exempel1	2020-08-31 00:11:10

Figur 3 – Exempel korrigering av tidszonsdifferens – originaltid.

Konvertering till svensk sommartid (UTC+2) sker genom addition av fem timmar:

	A	B	C	D	S
1	MESSAGE_TIME	MESSAGE_SENDER	MESSAGE_DECODED	MESSAGE_RECEIVER	MESSAGE_INSERTED
2	2020-08-27 22:48:46+0200	Exempel1	Hej	exempel2	2020-08-28 00:11:09
3	2020-08-27 22:50:01+0200	Exempel2	Hej på dig	Exempel1	2020-08-31 00:11:10
4	2020-08-27 22:50:15+0200	Exempel1	Hur går det?	Exempel2	2020-08-31 00:11:10
5	2020-08-27 22:51:04+0200	exempel2	Det går bra tack.	Exempel1	2020-08-31 00:11:10

Figur 4 – Exempel korrigering av tidszonsdifferens – korrekt svensk tid

I Polisens analysverktyg som hanterar och presenterar källmaterialet skedde automatisk korrigering av tidszon enligt ovan den 2021-09-30. Innan detta datum justerades samtliga tidsstämplar på meddelanden i analysverktyget från UTC till svensk tid vilket medför att urklipp och exporter av material som hämtats från analysverktyget innan 2021-09-30 presenterar tidsstämplar två till tre timmar felaktigt jämfört med svensk tid, beroende på i vilken tidsram det aktuella meddelandet blev inläst.

I källmaterialet har ingen tidszonsjustering utförts. Korrigerad tidsangivelse presenteras enligt ISO8601[3] där tidsangivelse presenteras med ett efterföljande plus- eller minustecken och tidszonsangivelse.

3.3.2 Tidzonsförskjutning 16-17 februari 2021

Det har i materialet identifierats ytterligare en tidzonsförskjutning för meddelanden skickade den 16 - 17 februari 2021. Detta förklaras genom att det vid den tiden förelåg ett problem i infrastrukturen som hanterade inläsning av nya meddelanden från servern i tredje land. På grund av detta skedde inläsning av nya data manuellt vilket kan ha orsakat tidzonsförskjutning på grund av mänsklig faktor. Exakt vilken tidzonsförskjutning det rör sig om och under vilka exakta tider har inte kunnat identifieras, men det finns flera exempel som tyder på att tidsstämpeln är satt två timmar efter att meddelandet i verkligheten skickats, exempelvis att ett meddelande har tidsstämpeln 17 feb 2021 01:21 (svensk tid) men i innehållet i meddelandena refererar de till att klockan är 23 (den 16 februari 2021). Efter den 17 februari 2021 åtgärdades problemen och tidsförskjutningen ser ut att upphöra någon gång under dagen den 17 februari 2021.

3.3.3 Övrig tidsförskjutning

Det har i materialet uppmärksammats en förskjutning i tid som yttrar sig på så sätt att vissa meddelandens tidsstämpel är satt 5–10 minuter innan meddelandet faktiskt har skickats.

Det har uppmärksammats genom analys av bilder där en tidsstämpel kunnat uppfattas, t.ex. bilder på klockor eller mobiltelefoner med synlig klocka samt genom matchning av tidsangivelsen i vidarebefordrade meddelanden och deras original.

Vid djupare analys har följande uppmärksammats:

- Från juni till slutet av augusti är differensen mellan fem och sju minuter.
- Från slutet av augusti till slutet av september är differensen oftast åtta minuter.
- Från slutet av september till den 7 oktober är differensen nio minuter.
- Från den 8 oktober till den 15 december är differensen tio minuter.
- Den 15 december 2020 upphör differensen.

3.3.3.1 Exempel övrig tidsförskjutning

Ett meddelande med tidsstämpel 2020-09-17 17:21:41 (svensk tid) innehåller en bild av en mobiltelefon där klockan visar 17:30, en differens på ca 8 minuter. Meddelandet bör därför i verkligheten ha skickats åtta minuter senare än dess tidsstämpel visar.

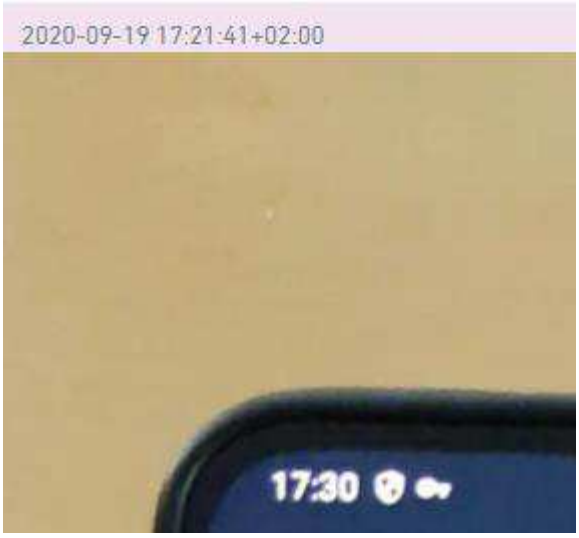


Fig 3. Tidsförskjutning exempel 1

Ett meddelande med tidsstämpel 2020-09-19 11:34:05 (svensk tid) innehåller en bild av en mobiltelefon där klockan visar 11:42, en differens på ca 8 minuter. Meddelandet bör därför i verkligheten ha skickats åtta minuter senare än dess tidsstämpel visar.

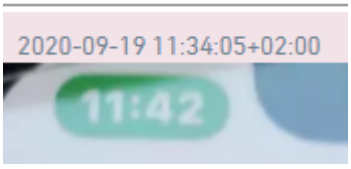


Fig 4. Tidsförskjutning exempel 2

3.4 Shmid är gemensamt för meddelanden och deras attachments

Enligt filen ”*data_information.txt*” ([5] Bilaga 1) framgår det att shmid skall vara ett UUID. Det har uppmärksammats i databaserna att flera rader kan ha samma shmid. Detta uppstår när ett bild-, text- eller ljudmeddelande är en bilaga (eng. attachment) till ett annat meddelande. Vid denna situation får samtliga meddelanden samma unika shmid. Meddelande-id, Mid, är alltid unikt för ett unikt meddelande.

3.5 Platsinformation

3.5.1 Tillförlitlighet MCC

För enheter innehållandes ett aktivt SIM-kort som var uppkopplat mot ett mobilnät försågs det skickade meddelandet med aktuell Mobile Country Code (MCC) för den sändande enheten (Appendix 8.2c [1]). En jämförelse av denna MCC mot textinnehåll samt GPS-position ger att denna MCC inte alltid är helt tillförlitlig. Detta yttrar sig som en fördröjning av byte mellan äldre MCC till ny MCC när enheten färdas från ett land till ett annat.

3.5.1.1 Exempel MCC

Nedan tabell innehåller exempel på koordinater och MCC från meddelanden där plats och MCC inte överensstämmer.

Message - Mcc	Message – Longitude	Message - Latitude	Land – MCC	Land - Koordinater
240	-4.511279	36.599588	Sverige	Spanien
240	-4.511137	36.599613	Sverige	Spanien
240	-4.511137	36.599613	Sverige	Spanien
240	-4.511226	36.599503	Sverige	Spanien
240	-4.621791	36.544923	Sverige	Spanien
240	-4.511296	36.599615	Sverige	Spanien
240	-4.511596	36.599373	Sverige	Spanien
240	-4.511298	36.599735	Sverige	Spanien

3.5.2 Misslyckad positionering – Felaktig Longitud

Efter en uppdatering i april 2020 försökte Anom-applikationen få fram enhetens position i samband med att meddelanden skickades. Detta kunde ibland misslyckas (*OTS A.8.2.d*), vilket resulterade i positionsvärden på följande vis:

Värdet för latitud är satt till ett heltal, t.ex. 59.0.

Värdet för longitud är satt till ett mycket stort tal, t.ex. 1617786553.

Värdet för longitud är vid det tillfället troligen en tidsstämpel i Unix Time.

3.5.2.1 Exempel misslyckad positionering – Felaktig longitud

Nedan tabell visar på exempel där meddelandets position visas felaktigt. Observera att bokstaven E i detta fall symboliserar multiplikation med den specificerade tiopotensen. 1.616779411E12 skall tolkas som $1.616779411 \times 10^{12}$.

Message – Time	Message - Longitude	Message - Latitude
2021-03-26 17:23:42+0100	1.616779411E12	59.0
2021-03-26 17:54:17+0200	1.617206019E12	59.0
2021-03-26 20:57:19+0100	1.616529358E12	59.0
2021-03-26 20:59:04+0100	1.61652912E12	59.0
2021-03-30 15:16:22+0100	1.616508937E12	59.0
2021-04-07 13:20:54+0200	1.617794386E12	59.0
2021-04-24 14:58:07+0100	1.616594251E12	59.0

3.5.3 Misslyckad positionering – Trunkerade koordinater

Ett annat förekommande exempel på hur positionering har misslyckats kan ses genom trunkering av värdet på koordinater i materialet. Denna trunkering yttrar sig genom att värdet för longitud trunkeras från vänster och saknar värde för heltal. Det värde som presenteras är istället värdet på decimalerna. På liknande men omvänt sätt har värdet för latitud trunkerats från höger och saknar värde för decimalerna. Det värde som presenteras är enbart värdet på heltalet.

3.5.3.1 Exempel misslyckad positionering – Trunkerade koordinater

Nedan tabell visar på exempel där meddelandets position visas felaktigt. Observera att enheten i det här fallet delvis rapporterat korrekta koordinater, 29.008981, 41.078515 och delvis trunkerade dito, 8981.0, 41.0. Se även fig 5 för en visualisering över trunkeringen.

Message - Time	Message - Longitude	Message - Latitude
2020-10-16 10:26:38+0200	8981.0	41.0
2020-10-16 10:26:53+0200	8981.0	41.0
2020-10-16 10:27:47+0200	29.008981	41.078515
2020-10-16 10:28:11+0200	29.008981	41.078515
2020-10-16 10:28:14+0200	29.008981	41.078515
2020-10-16 13:42:53+0200	8476.0	41.0
2020-10-16 13:42:54+0200	8476.0	41.0

Kommentar	Message - Latitude	Message - Longitude	Message - Time
Trunkerade koordinater	41.0	8981.0	2020-10-16 10:26:38+0200
Trunkerade koordinater	41.0	8981.0	2020-10-16 10:26:53+0200
Korrekta koordinater	41.078515	29.008981	2020-10-16 10:27:47+0200
Korrekta koordinater	41.078515	29.008981	2020-10-16 10:28:11+0200
Korrekta koordinater	41.078515	29.008981	2020-10-16 10:28:14+0200
Trunkerade koordinater	41.0	8476.0	2020-10-16 13:42:53+0200
Trunkerade koordinater	41.0	8476.0	2020-10-16 13:42:54+0200

Fig 5. Trunkerade koordinater, visualisering över trunkering.

3.5.4 Positionering visar tidigare känd plats

När position hämtas via Android Location Manager kan hämtningen i vissa fall misslyckas varpå den senast kända positionen hämtas istället. Detta beskrivs i detalj i dokumentet ”Positionsdata i meddelanden skickade med applikationen ANØM”, A673.978/2021.

3.5.4.1 Exempel positionering visar tidigare känd plats

Nedan meddelanden visar på ett tillfälle då enhetens position inte kunnat uppdateras. Klockan 13:49 fastställs positionen till 16.489885, 59.596813. Enheten har sedan dess flyttats (enligt annan information i utredningen) men ny position registreras inte förrän klockan 18:50.

Message - Time	Message - Longitude	Message - Latitude
2021-05-19 13:49:19+0200	16.489735	59.596842
2021-05-19 13:49:39+0200	16.489885	59.596813
2021-05-19 13:50:23+0200	16.489885	59.596813
2021-05-19 17:32:59+0200	16.489885	59.596813
2021-05-19 18:04:08+0200	16.489885	59.596813
2021-05-19 18:50:33+0200	17.221353	59.640529
2021-05-19 18:52:16+0200	17.161794	59.64619

3.6 MDM och Roster – Statisk information

Innehåll i tabeller MDM och Roster innehåller den senast kända informationen. En användare av Anom kan använda sig av flera olika enheter med skilda IMEI-nummer såväl som olika SIM-kort. Tabellerna Roster och MDM innehåller den information som var aktuell vid slutet av operation Trojan Shield. Den kompletterande MDM-informationen som behandlas i kap 2.2.6.1 innehåller samtliga kombinationer av enheter aktuellt JID brukat.

Under operation Trojan Shield försågs Polismyndigheten med datapaket varje måndag, onsdag och fredag. Datapaketen innehöll samtliga meddelanden genererade sedan den senaste exporten. Meddelanden var försedda med det alias aktuellt JID hade vid exporttillfället. Det resulterar i att byten av alias i regel visas i materialet upp till tre dagar *tidigare* än de i verkligheten skett. I vissa fall har det observerats att ett nytt alias inte visas i materialet förrän flera veckor *efter* att bytet i verkligheten har skett. På grund av att alias endast kontrollerades vid specifika tillfällen är det möjligt att vissa alias saknas i materialet.

3.7 Användandet av flera enheter

Vid initial uppsättning av ett nytt användarkonto i Anom genererade en återförsäljare ett unikt JID som kontrollerades mot en databas för att säkerställa att JID var unik och inte tidigare brukats inom Anom. Efter att det nya användarkontot satts upp tillhandahölls ett nytt lösenord till återförsäljaren.

Efter att en brukare av JID loggat in på en enhet ändrades det ursprungliga lösenordet till ett slumpmässigt genererat 256 tecken långt nytt lösenord.

Innan uppdatering till Android 10 som skedde under december 2020 var det inte möjligt för ett JID att logga in på en annan enhet än den som initialt sattes upp av återförsäljare eller administratör.

Från och med denna uppdatering var det möjligt för ett JID att använda sig av en annan enhet än den som initialt satts upp till detta JID.

För att kunna logga in på ytterligare en enhet krävdes att en återförsäljare först nollställde lösenordet. Vid nollställning av lösenordet blev eventuell redan inloggad enhet utloggad efter fem minuters inaktivitet och nekad möjligheten att logga in på nytt.

Mellan januari till mars 2021 var det möjligt för ett JID att vara inloggat på två enheter samtidigt, förutsatt att:

- En administratör eller återförsäljare återställde lösenordet för aktuell JID innan varje ny inloggning.
- Att den första enheten var aktiv så att den automatiska utloggningen inte skedde.
- Att enheten var uppdaterad till Android 10 eller senare.

Att en och samma JID var inloggad på två enheter var en sällsynt företeelse som vanligtvis orsakades av en oerfaren återförsäljare som var obekant med återställningsprocessen.

I slutet av mars 2021 justerades lösningen för att förhindra att ett och samma JID kunde använda fler enheter samtidigt. Uppdateringen innebar att en eventuell redan aktiv enhet loggades ut i samma ögonblick som en ny enhet loggades in. *OTS Bilaga Klonade enheter*

3.8 Användaren bot

Applikationen Anom innehöll en funktion som innebar att när ett meddelande skickades så skickades det även automatiskt en dold kopia av meddelandet till en dold/fiktiv användare med användarnamnet ”bot”. Den här processen var inte synlig för den användare som skickade meddelandet, och den användaren visste inte heller om att processen ägde rum. *OTS Kap 1. ÖVERSIKT ÖVER SERVRAR OCH NÄTVERK.*

Under perioden 2021-05-05 – 2021-06-07 förekommer det i materialet meddelanden adresserade till användaren ”bot”. Detta beror på en felaktig uppdatering av Anom som drogs tillbaka.

4 Källförteckning

[1] https://polisen.se/aktuellt/nyheter/2021/juni/155-frihetsberovade-i-storsta-insatsen-hittills-mot-organiserad-brottslighet/ [Hämtat 2021-10-07]

[2] Teknisk information om Operation Trojan Shield [Översatt version, senast uppdaterad 31 augusti 2021]

[3] https://www.iso.org/iso-8601-date-and-time-format.html [Hämtat 2021-12-16]

[4] https://xmpp.org/rfcs/rfc3921.html#session [Hämtat 2021-12-29]

[5] A605.844/2021 Beskrivning av Polismyndighetens hantering av Anom-data

A605.844/2021

polisen.se

Polisens IT-avdelning

Telefon 114 14

e-post registrator@polisen.se

Polisen

A605.844/2021

IT-avdelningen

Anom

Beskrivning av Polismyndighetens hantering av Anom-data

Rapport

Utgivare
Polismyndigheten
Tfn 114 14
E-post kansli.registrator@polisen.se
www.polisen.se

Produktion Polismyndigheten, 2021-09-21
Upplaga [XX] ex

Diarienr. AXX
Tryck Polisens tryckeri

Sammanfattning

Detta dokument innehåller en beskrivning av Polismyndighetens metod och hantering av materialet som inkommit i operation Trojan Shield som berör avkrypterad information från kommunikationstjänsten Anom.

Information har inkommit i form av hårddiskar, där varje hårddisk innehåller data från en gruppering av användare, även kallat syndikat.

Ovan nämnda databaser innehåller meddelanden och bilagor dessa användare skickat i plattformen. Dessa databaser är även försedda med metadata kring dessa meddelanden och användare.

Dokumentet beskriver materialets format och struktur. Information om själva innehållet, den dekrypterade informationen beskrivs i dokumentet *”Beskrivning av information i Anom-data”*

I detta dokument finns flertalet hänvisningar till dokumentet *”Teknisk information om Operation Trojan Shield”* som vidare beskriver materialet och dess hantering innan det kom Polismyndigheten till handa.

Innehållsförteckning

1 Inledning

1.1 Bakgrund

Sammanlagt har 16 länder världen över ingått i insatsen som gått under namnet Trojan Shield/OTF Greenlight. I Europa har arbetet letts av Sverige och Nederländerna i samarbete med Europol.
Den krypterade plattformen Anom, som nu har avvecklats, har använts av kriminella för att planera, koordinera och kunna utföra brott.

Plattformen skapades och administrerades i det dolda av FBI. I takt med att liknande tjänster som ”*Encrochat*” och ”*Sky ECC*” upphörde övergick allt fler kriminella aktörer till att kommunicera på denna plattform.

Enligt FBI har över 27 miljoner meddelanden skickats via plattformen av över 200 kriminella nätverk mellan oktober 2019 och juni 2021. [1]

Efter att plattformen avvecklades i juni 2021 har Polismyndigheten av FBI försetts med exporter av meddelanden och annan information från plattformen i enlighet med det ömsesidiga juridiska biståndsavtalet (MLAT) mellan USA och EU.

1.2 Syfte

Dokumentet syftar till att beskriva innehållet i de exporter FBI försett polismyndigheten med samt hur dessa har behandlats inom Polisen. Dokumentet beskriver även hur extrahering av information ur exporter för hantering inom FU genomförts.

1.2.1 Avgränsning

Dokumentet syftar inte till att beskriva innehåll i exporter. Detta sker i det separata dokumentet ”*Beskrivning av information i Anom-data”*

1.3 Hänvisning till OTS Technical Details

I detta dokument finns flertalet hänvisningar till det tekniska dokument som är framtaget för Operationen Trojan Shield (OTS) [2]. Det tekniska dokumentet finns i en engelsk och i en svensk version. Hänvisning till respektive kapitel och eventuellt avsnitt är detsamma i både det svenska och det engelska dokumentet. För tydlighetens skull kommer dessa hänvisningar betecknas med kursiv stil *OTS kap. <kapitel>.<avsnitt> <svensk rubrik>*. Exempelvis: *OTS kap. 8.1 Ärenden/syndikat.*

2 MLAT exporter

Material som begärts från USA via MLAT har inkommit som enheter (externa hårddiskar och USB-enheter) med exporter. Dessa har skickats till Sverige och mottagits av Justitiedepartementet och/eller Åklagarmyndighetens Riksenhet mot internationell och organiserad brottslighet (RIO). Dessa enheter har sedan vidarebefordrats till Polismyndigheten för fortsatt hantering. För mer information om MLAT-exporter se *OTS kap. 11 MLAT-export*.

2.1 Beskrivning och hantering av fysiskt media

Polismyndigheten har totalt mottagit åtta externa hårddiskar och fyra USB-minnen innehållandes rådata.

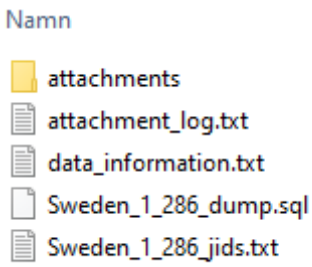
Samtliga enheter har efter ankomst speglats och hanterats enligt gängse rutiner av IT-forensik 1, Utredningsenheten, Polisregion Stockholm.

2.2 Innehåll fysiskt media

Varje fysiskt media utgör en export av ett så kallat syndika. För ytterligare information om syndikat och dess uppdelning hänvisas till *OTS kap. 8.1 Ärenden/syndikat*. De 8 externa hårddiskarna utgör initiala exporter och de 4 USB-minnen utgör tilläggsexporter för vissa syndikat.

För varje enhet finns denna uppsättning av filer

- En katalog innehållandes bilagor i form av ljud-, video-, och bildmaterial (Attachments).
- Information om vilka bilagor som förekommer i ovan katalog (attachment_log.txt).
- Beskrivning av dataformatet (data_information.txt).
- Instruktioner för upprättande av databas (Sweden_<*syndikat*>_dump.sql)
- En förteckning av de
- Information om vilka bilagor som förekommer.



Figur 1. Exempel på filstruktur innehåll, syndikat 286

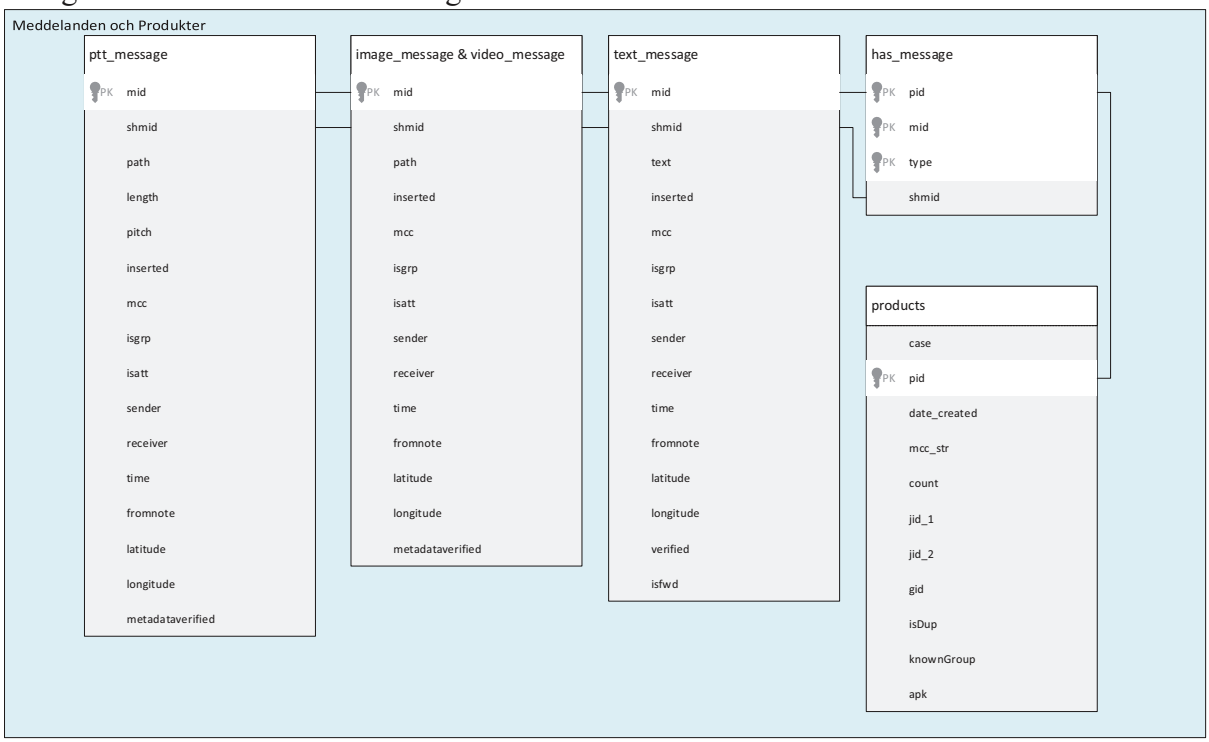
2.2.1 Maskininstruktioner

I filen Sweden<syndikat>_dump.sql återfinns instruktioner för att skapa en MySQL[3]-databas innehållandes följande tabeller:

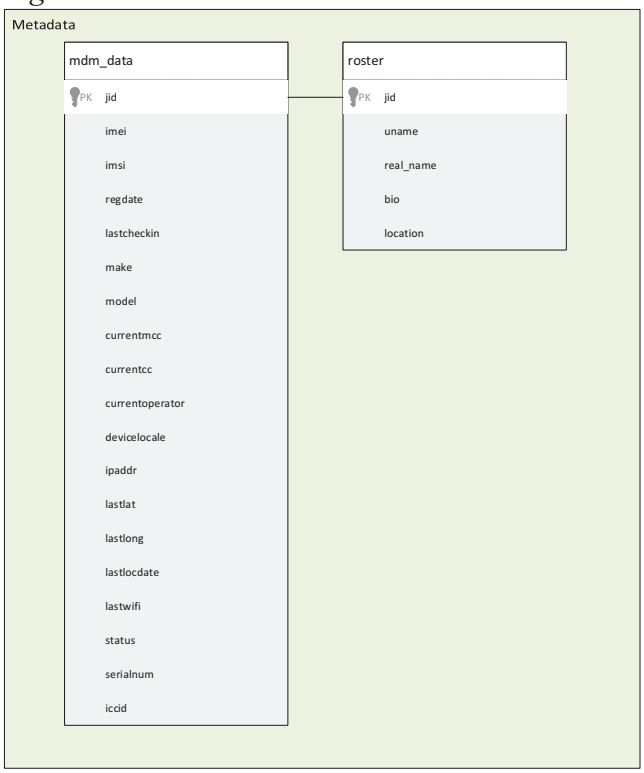
- Has_message
- Image_message
- Mdm_data
- Products
- Ptt_message
- Roster
- Text_message
- Video_message

I filen ”*data_information.txt*” (bilaga 1) återfinns fördjupad information om tabellernas struktur och innehåll. Detta fördjupas ytterligare i *OTS kap.8 Databasöversikt*

Se figur 2 och 3 för en visualisering av databas-strukturen samt dess relationer



Figur 2 Databasstruktur meddelanden



Figur 3 Databasstruktur metadata

2.2.2 Bifogade filer

I katalogen attachments återfinns tre underordnade kataloger

- Audio

- Video
- Images

I dessa finns all media som skickats i konversationer som attribuerats till syndikatet.

I filen ”*attachment_log.txt*” återfinns information om huruvida exporten av media tillhörande syndikatet har lyckats eller misslyckats. Totalt sett har 192 bilagor misslyckats.

2.2.3 Metadata

I filen ”*Sweden_<syndikat>_jids.txt*” återfinns samtliga s.k. Jabber Identification, även förkortat till JID, som attribuerats till syndikatet.

3 Delningsförfarande

Efter delningsbeslut av exportägande åklagare registreras vilken/vilka JID/s det specifika ärendet skall ta del av. Därefter delas följande information:

- Samtliga meddelanden från samtliga konversationer där aktuell JID deltar som sändare eller mottagare.
- MDM-information om aktuell JID.
- Roster-information om aktuell JID.

4 Behandling av information

4.1 Extrahering från databas per JID

Efter delningsbeslut från exportägande åklagare genomförs ett antal databasfrågor mot de olika databaserna. Exempel på dessa databasfrågor återfinns i bilaga 3.

4.2 Filformat – TSV

Samtliga databasfrågor blir sedan presenterade i ett antal tabb-separerade filer som sparas med filändelsen ”.tsv”. Dessa kan öppnas i valfritt program för textbehandling och beskrivs mer detaljerat nedan.

4.3 Textkodning i Base64

Textmeddelanden lagras som en BLOB (Binary Large OBject) [4] i databasen. Vid export konverteras detta till Base64 [5], vilket är en textbaserad representation av det binära objektet. Ingen information går förlorad vid denna konvertering.

4.4 Hänvisning till Media

För varje enskilt meddelande som innehåller media finns en referens till motsvarande fil i MLAT-exportens attachments-katalog.

4.5 Deduplicering av meddelanden

Deduplicering är en form av komprimering i syfte att endast presentera unikt data. Meddelanden från Anom har kunnat deduplicerats så att läsare av dessa endast behövt se varje unikt meddelande en gång. Fördjupning och tillvägagångssätt presenteras nedan.

4.5.1 Anledning till deduplicering

En enskild konversation kan förekomma i flera av de exporterade databaserna. Detta beror oftast på att deltagande JID:ar ingår i flera syndikat vilket medför att flera identiska kopior av konversationer förekommer för dessa JID:ar

4.5.2 Metod

Varje enskilt meddelande är försett med ett unikt meddelande-id (”mid”). Eftersom det unika meddelandet förekommer flera gånger blir dessa kombinerade till endast en rad med hänvisning till vilka konversationer/produkter detta meddelande deduplicerats ifrån.

4.5.3 Verifiering

En kontroll av att varje duplicerad konversation innehåller exakt samma meddelanden har genomförts.

4.6 Alias-information

Användare av Anom kan förse sin JID med ett eget Alias. Information om vilket Alias en JID använt sig av återfinns i Roster-tabellen. Att observera är att denna information är den som var aktuell vid slutfasen av Operation Trojan Shield.

En användare av Anom kan använt sig av andra Alias än detta historiskt.

Under operation Trojan Shield försågs Sverige löpande med meddelanden exporterade från ”hola iBot” *OTS kap.9.5 Export efter inmatning.* Dessa exporter skedde måndagar, onsdagar och fredagar. Meddelanden i exporter innehåller information om vilket Alias aktuell JID använt vid export-tillfället. Om en JID bytt Alias flera gånger mellan exporttillfällen har detta inte kunnat fastställas.

Efter deduplicering av innehållet har därför varje enskilt meddelande som avsänts från en i ärendet förekommande JID kunnat förses med det Alias JID:en använt för detta meddelande.

4.7 Dekodning och presentation av källmaterial

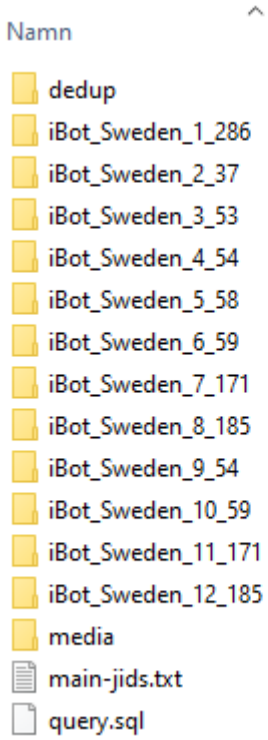
Samtliga TSV-filer med rådata från databasexport och all hänvisat media har levererats till förundersökning för vidare analys.

Förutom detta har även resultatet av deduplicering och Alias-information levererats i egna TSV-filer.

För att underlätta läsning av materialet har varje TSV-fil konverterats till Excel-format. I detta har Base64-texten konverterats till läsbar text samt länkar till hänvisat media infogats. Dessa Excel-filer har även försetts med en rubrikrad. Följande kataloger och filer återfinns:

- En katalog per databas där material extraherats. Dessa har försetts med löpnummer 1-12.
- En katalog med resultat av deduplicering och Alias-innehåll.
- En katalog innehållandes media som aktuell JID skickat och tagit emot

- En text-fil ”main-jids.txt” där aktuell JID framgår.
- En sql-fil ”query.sql” som innehåller den databasfråga som ställts för att generera TSV-filer.



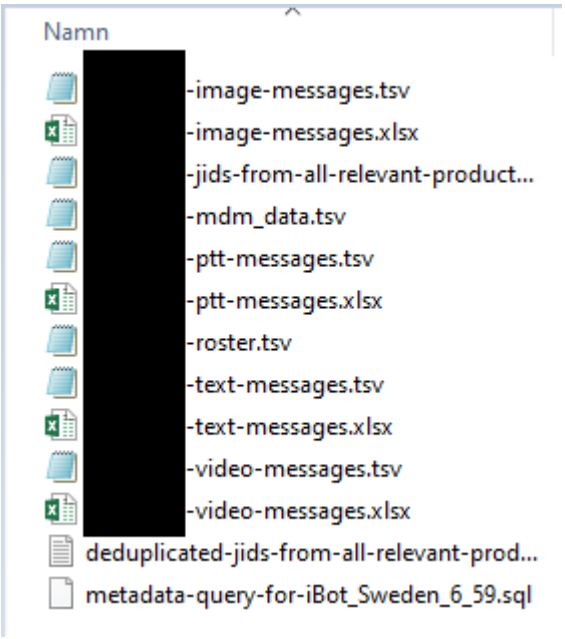
Figur 4 Katalogstruktur exporter

Nedan följer en beskrivning av innehållet i ovan nämnda kataloger.

4.7.1 Per databas

Följande filer återfinns i varje katalog med databasexporter. Dessa finns alltid som TSV oavsett om filen har innehåll eller inte och är ett direkt resultat av databasexport.

Om filen har innehåll har det även skett en konvertering till ett format som är läsbart i Excel. I de fallen har varje fält försetts med en rubrikrad.



Figur 5 Innehåll per databas för en JID. Denna JID har maskerats.

Kolumnerna är uppbyggda på följande vis:

<TABELL>_<FÄLT>

T.ex. innehåller kolumnen “HAS_MESSAGE_MID” fältet ”*mid*”, hämtat från tabellen ”*has_message*” i aktuell databas. Fördjupad information om innehållet i fälten återfinns i [1]

Nedan återfinns beskrivning över innehåll i TSV-filer. Dessa fält är tabb-separerade. Om ett värde inte finns för fältet representeras detta med ”\N”.

I Excel-versioner av dokumenten har informationen försetts med rubrikrad. I Excelfiler innehållandes meddelanden har hänvisning till media försetts med klickbar hyperlänk till aktuellt media.

För fältordning i TSV-filer, se bilaga 2.

4.7.1.1 <JID>-image-messages & <JID>-video-messages

Innehåller samtliga meddelanden och metadata innehållandes bild- respektive videomaterial där aktuell JID varit sändare eller mottagare.

4.7.1.2 <JID>-text-messages

Innehåller samtliga meddelanden och metadata innehållandes text-material där aktuell JID varit sändare eller mottagare.

4.7.1.3 <JID>-ptt-messages

Innehåller samtliga meddelanden och metadata innehållandes ljud-material där aktuell JID varit sändare eller mottagare.

4.7.1.4 <JID>-jids-from-all-relevant-products

Innehåller samtliga JID:ar som förekommer i exporterat material. Denna information återfinns även deduplicerat i en separat textfil ”deduplicated-jids-from-all-relevant-products.txt”

4.7.1.5 <JID>-mdm_data

Innehåller samtlig tillgänglig Mobile Device Management-information för aktuell JID

4.7.1.6 <JID>-roster

Innehåller samtlig tillgänglig roster-information för aktuell JID

4.7.1.7 Metadata-query-for-<databas>.sql

Innehåller den SQL-fråga som ställts mot aktuell databas för att extrahera informationen till Roster och MDM.

4.7.2 Dedup

I katalogen dedup återfinns resultatet av deduplicering och tillfogande av Alias-information på meddelanden. I de fall ett deduplicerat meddelande har flera värden i något av fälten är dessa separerade med semikolon. Fältrubriker i TSV-filer är identiska med de icke deduplicerade filerna. En kolumn ”SENDER_ALIAS” har lagts till efter ordinarie kolumner i varje fil. Denna kolumn innehåller det Alias den JID som är aktuell för exporten använt i enlighet med kap 4.6.
I katalogen finns även en fil *main-alias.tsv* som innehåller tre kolumner:

- Alias
- JID
- mid

Detta är en förteckning över samtliga Alias aktuell JID använt på aktuellt meddelande (mid). Denna är samma mid som återfinns i kolumnerna
HAS_MESSAGE_MID
MESSAGE_MID

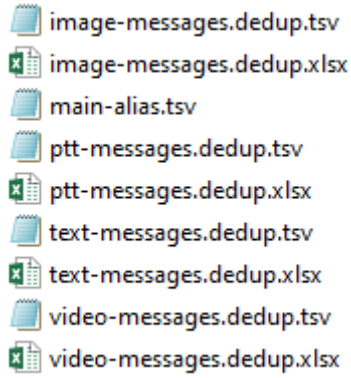


Fig 6, Innehåll dedup

En eventuell felkälla till dessa Alias är om aktuell JID bytt Alias under tiden mellan exporter har detta inte registrerats, se 4.6

4.7.3 Media

Innehåller tre kataloger, audio, images, videos. Dessa innehåller de ljudklipp, bilder och filmklipp som har skickats i meddelanden. Dessa hänvisas till genom ett Universally Unique IDentifier (UUID) [6]

5 Källförteckning

[1] https://polisen.se/aktuellt/nyheter/2021/juni/155-frihetsberovade-i-storsta-insatsen-hittills-mot-organiserad-brottslighet/ [Hämtat 2021-10-07]

[2] Teknisk information om Operation Trojan Shield [Översatt version, senast uppdaterad 31 augusti 2021]

[3] MySQL 8.0 Reference Manual, What is MySQL? https://dev.mysql.com/doc/refman/8.0/en/what-is.html [Hämtat 2021-09-21]

[4] MySQL 8.0 Reference Manual, Data Types https://dev.mysql.com/doc/refman/8.0/en/blob.html [Hämtat 2021-09-21]

[5] IETF RFC 3548, https://datatracker.ietf.org/doc/html/rfc3548 [Hämtat 2021-09-21]

[6] IETF RFC 4122, https://datatracker.ietf.org/doc/html/rfc4122 [Hämtat 2021-09-23]

6 Bilagor

Bilaga 1 – Data_information.txt

The following is information about the data stored on this drive.

Contained on this drive are the following files/directories:

- data_information.txt
- <countryname_number>_jids.txt
- <countryname_number>_dump.sql
- attachments/
  - images
  - videos
  - audio

The attachment_log.txt contains the attachments that were included in the export. If 'success' is shown next to the attachment filename, this means the attachment will be in the attachments directory. If 'failure' is next to the attachment filename, we do not have the attachment.

The sql dump contains the following schema, this has been commented explaining the fields, many of the fields are replicated or obvious:

```
CREATE TABLE `has_message` (
  `pid` int(11) NOT NULL,                    //product ID
  `mid` int(11) NOT NULL,                    //message ID
  `type` varchar(20) NOT NULL,               //1 is text, 2 is image, 3 is ptt, 4 is video
  `shmid` varchar(50) DEFAULT NULL,
 PRIMARY KEY (`pid`,`mid`,`type`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;

CREATE TABLE `image_message` (
  `mid` int(11) NOT NULL,                          //message ID
  `shmid` varchar(50) NOT NULL,                    //message UUID
  `path` varchar(100) NOT NULL,                    //image file name
  `inserted` timestamp NOT NULL DEFAULT current_timestamp(),
  `mcc` varchar(20) NOT NULL,
  `isgrp` int(2) NOT NULL DEFAULT 0,               //if it's from a group message
  `isatt` int(2) NOT NULL DEFAULT 0,
  `sender` varchar(50) NOT NULL,
  `receiver` varchar(50) NOT NULL,
  `time` timestamp NOT NULL DEFAULT current_timestamp(),
  `fromnote` int(2) NOT NULL DEFAULT 0,            //if it's from a note attachemt
  `latitude` varchar(512) DEFAULT NULL,
  `longitude` varchar(512) DEFAULT NULL,
```

```
  `metadataverified` int(2) NOT NULL DEFAULT 0,
  PRIMARY KEY (`mid`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
CREATE TABLE `mdm_data` (
  `jid` varchar(50) NOT NULL,
  `imei` varchar(50) DEFAULT NULL,
  `imsi` varchar(50) DEFAULT NULL,
  `regdate` timestamp NOT NULL DEFAULT '0000-00-00 00:00:00',
  `lastcheckin` timestamp NOT NULL DEFAULT '0000-00-00 00:00:00',
  `make` blob DEFAULT NULL,
  `model` blob DEFAULT NULL,
  `currentmcc` varchar(20) DEFAULT NULL,
  `currentcc` varchar(20) DEFAULT NULL,
  `currentoperator` blob DEFAULT NULL,
  `currentphone` varchar(20) DEFAULT NULL,
  `devicelocale` blob DEFAULT NULL,
  `ipaddr` varchar(50) DEFAULT NULL,
  `lastlat` varchar(512) DEFAULT NULL,
  `lastlong` varchar(512) DEFAULT NULL,
  `lastlocdate` timestamp NOT NULL DEFAULT '0000-00-00 00:00:00',
  `lastwifi` blob DEFAULT NULL,
  `status` varchar(512) DEFAULT NULL,
  `serialnum` varchar(50) DEFAULT NULL,
  `iccid` varchar(100) DEFAULT NULL,
  PRIMARY KEY (`jid`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1;
CREATE TABLE `products` (
  `case_id` int(11) NOT NULL,                    //syndicate ID
  `pid` int(20) NOT NULL AUTO_INCREMENT,         //product ID
  `date_created` timestamp NOT NULL DEFAULT current_timestamp(),
  `mcc_str` blob NOT NULL,
  `jid_str` blob NOT NULL,
  `count` int(11) NOT NULL DEFAULT 0,            //num messages in product
  `jid_1` varchar(50) DEFAULT NULL,
  `jid_2` varchar(50) DEFAULT NULL,
```

```
  `gid` varchar(100) DEFAULT 'NULL',
  `isDup` int(2) NOT NULL DEFAULT 0,                    //is it a duplicate product
  `knownGroup` int(11) DEFAULT NULL,
  `apk` varchar(100) DEFAULT NULL,
  PRIMARY KEY (`pid`),
  KEY `idx_products_pid` (`pid`),
  KEY `idx_products_jid1` (`jid_1`),
  KEY `idx_products_jid2` (`jid_2`)
) ENGINE=InnoDB AUTO_INCREMENT=677525 DEFAULT CHARSET=utf8mb4;
CREATE TABLE `ptt_message` (
  `mid` int(11) NOT NULL,
  `shmid` varchar(50) NOT NULL,
  `path` varchar(100) NOT NULL,
  `length` varchar(20) DEFAULT NULL,
  `pitch` varchar(10) NOT NULL,                         //original pitch of the ptt message
  `inserted` timestamp NOT NULL DEFAULT current_timestamp(),
  `mcc` varchar(20) NOT NULL,
  `isgrp` int(2) NOT NULL DEFAULT 0,
  `isatt` int(2) NOT NULL DEFAULT 0,
  `sender` varchar(50) NOT NULL,
  `receiver` varchar(50) NOT NULL,
  `time` timestamp NOT NULL DEFAULT current_timestamp(),
  `latitude` varchar(512) DEFAULT NULL,
  `longitude` varchar(512) DEFAULT NULL,
  `metadataverified` int(2) NOT NULL DEFAULT 0,
  PRIMARY KEY (`mid`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
CREATE TABLE `roster` (
  `jid` varchar(50) NOT NULL,
  `uname` blob NOT NULL,          //user assigned name
  `real_name` blob DEFAULT NULL,  //attribuited name by monitors
  `bio` blob DEFAULT NULL,
  `location` blob DEFAULT NULL,
  PRIMARY KEY (`jid`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
```

```
CREATE TABLE `text_message` (
  `mid` int(11) NOT NULL,
  `shmid` varchar(50) NOT NULL,
  `text` mediumblob NOT NULL,                //text of the message
  `inserted` timestamp NOT NULL DEFAULT current_timestamp(),
  `mcc` varchar(20) NOT NULL,
  `isgrp` int(2) NOT NULL DEFAULT 0,
  `isatt` int(2) NOT NULL DEFAULT 0,
  `sender` varchar(50) NOT NULL,
  `receiver` varchar(50) NOT NULL,
  `time` timestamp NOT NULL DEFAULT current_timestamp(),
  `fromnote` int(2) NOT NULL DEFAULT 0,
  `latitude` varchar(512) DEFAULT NULL,
  `longitude` varchar(512) DEFAULT NULL,
  `verified` int(2) NOT NULL DEFAULT 0,
  `isfwd` int(2) NOT NULL DEFAULT 0,
  PRIMARY KEY (`mid`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
CREATE TABLE `video_message` (
  `mid` int(11) NOT NULL,
  `shmid` varchar(50) NOT NULL,
  `path` varchar(100) NOT NULL,
  `inserted` timestamp NOT NULL DEFAULT current_timestamp(),
  `mcc` varchar(20) NOT NULL,
  `isgrp` int(2) NOT NULL DEFAULT 0,
  `isatt` int(2) NOT NULL DEFAULT 0,
  `sender` varchar(50) NOT NULL,
  `receiver` varchar(50) NOT NULL,
  `time` timestamp NOT NULL DEFAULT current_timestamp(),
  `latitude` varchar(512) DEFAULT NULL,
  `longitude` varchar(512) DEFAULT NULL,
  `metadataverified` int(2) NOT NULL DEFAULT 0,
  PRIMARY KEY (`mid`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
```

Bilaga 2 – Fältordning TSV-Filer

<JID>-image-messages & <JID>-video-messages

Följande fältordning återfinns i TSV-fil:
HAS_MESSAGE_PID
HAS_MESSAGE_MID
HAS_MESSAGE_TYPE
HAS_MESSAGE_SHMID
MESSAGE_MID
MESSAGE_SHMID
MESSAGE_PATH
MESSAGE_INSERTED
MESSAGE_MCC
MESSAGE_ISGRP
MESSAGE_ISATT
MESSAGE_SENDER
MESSAGE_RECEIVER
MESSAGE_TIME
MESSAGE_FROMNOTE
MESSAGE_LATITUDE
MESSAGE_LONGITUDE
MESSAGE_METADATAVERIFIED
PRODUCTS_CASE_ID
PRODUCTS_PID
PRODUCTS_DATE_CREATED
PRODUCTS_MCC_STR
PRODUCTS_JID_STR
PRODUCTS_COUNT
PRODUCTS_JID_1
PRODUCTS_JID_2
PRODUCTS_GID
PRODUCTS_ISDUP
PRODUCTS_KNOWNGROUP
PRODUCTS_APK

<JID>-text-messages

Följande fältordning återfinns i TSV-fil:
HAS_MESSAGE_PID
HAS_MESSAGE_MID
HAS_MESSAGE_TYPE
HAS_MESSAGE_SHMID
MESSAGE_MID
MEE_SHMID
MESSAGE_CONTENT
MESSAGE_INSERTED
MESSAGE_MCC
MESSAGE_ISGRP
MESSAGE_ISATT
MESSAGE_SENDER
MESSAGE_RECEIVER
MESSAGE_TIME
MESSAGE_FROMNOTE
MESSAGE_LATITUDE
MESSAGE_LONGITUDE
MESSAGE_METADATAVERIFIED
MESSAGE_ISFWD
PRODUCTS_CASE_ID
PRODUCTS_PID
PRODUCTS_DATE_CREATED
PRODUCTS_MCC_STR
PRODUCTS_JID_STR
PRODUCTS_COUNT
PRODUCTS_JID_1
PRODUCTS_JID_2
PRODUCTS_GID
PRODUCTS_ISDUP
PRODUCTS_KNOWNGROUP
PRODUCTS_APK

<JID>-ptt-messages

Följande fältordning återfinns i TSV-fil:
HAS_MESSAGE_PID
HAS_MESSAGE_MID
HAS_MESSAGE_TYPE
HAS_MESSAGE_SHMID
MESSAGE_MID
MESSAGE_SHMID
MESSAGE_PATH
MESSAGE_LENGTH
MESSAGE_PITCH
MESSAGE_INSERTED
MESSAGE_MCC
MESSAGE_ISGRP
MESSAGE_ISATT
MESSAGE_SENDER
MESSAGE_RECEIVER
MESSAGE_TIME
MESSAGE_LATITUDE
MESSAGE_LONGITUDE
MESSAGE_METADATAVERIFIED
PRODUCTS_CASE_ID
PRODUCTS_PID
PRODUCTS_DATE_CREATED
PRODUCTS_MCC_STR
PRODUCTS_JID_STR
PRODUCTS_COUNT
PRODUCTS_JID_1
PRODUCTS_JID_2
PRODUCTS_GID
PRODUCTS_ISDUP
PRODUCTS_KNOWNGROUP
PRODUCTS_APK

<JID>-mdm_data

Följande fältordning återfinns i TSV-fil:
MDM_JID
MDM_IMEI
MDM_IMSI
MDM_REG_DATE
MDM_LAST_CHECKIN
MDM_MAKE
MDM_MODEL
MDM_CURRENT_MCC
MDM_CURRENT_CC
MDM_CURRENT_OPERATOR
MDM_CURRENT_PHONE
MDM_DEVICE_LOCALE
MDM_IPADDR
MDM_LAST_LAT
MDM_LAST_LONG
MDM_LAST_LOC_DATE
MDM_LAST_WIFI
MDM_STATUS
MDM_SERIAL_NUM
MDM_ICCID

<JID>-roster

Följande fältordning återfinns i TSV-fil:
JID
SENDER_ALIAS
REAL_NAME
BIO
LOCATION

Bilaga 3 Exempel databasfrågor

Vid varje enskild export av JID ställs följande frågor mot varje enskild databas. Resultatet flyttas sedan till tidigare beskrivna kataloger

Bild-meddelanden

```
SELECT *
FROM has_message
INNER JOIN image_message ON image_message.mid = has_message.mid
LEFT JOIN products ON has_message.pid = products.pid
WHERE convert(jid_str USING utf8) LIKE '%<JID>%'
INTO OUTFILE '/var/lib/mysql-files/<JID>-image-messages.tsv';
```

Ljud-meddelanden

```
SELECT *
FROM has_message
INNER JOIN ptt_message ON ptt_message.mid = has_message.mid
LEFT JOIN products ON has_message.pid = products.pid
WHERE convert(jid_str USING utf8) LIKE '%<JID>%'
INTO OUTFILE '/var/lib/mysql-files/<JID>-ptt-messages.tsv';
```

Text-meddelanden

```
SELECT has_message.pid, has_message.mid, has_message.type, has_message.shmid, text_message.mid,
text_message.shmid, TO_BASE64(text_message.text) AS base_64text, text_message.inserted,
text_message.mcc, text_message.isgrp, text_message.isatt, text_message.sender, text_message.receiver,
text_message.time, text_message.fromnote, text_message.latitude, text_message.longitude,
text_message.verified, text_message.isfwd, products.case_id, products.pid, products.date_created, prod-
ucts.mcc_str, products.jid_str, products.count, products.jid_1, products.jid_2, products.gid, products.isDup,
products.knownGroup, products.apk
FROM has_message
INNER JOIN text_message on text_message.mid = has_message.mid
LEFT JOIN products on has_message.pid = products.pid
WHERE convert(jid_str USING utf8) LIKE '%<JID>%'
INTO OUTFILE '/var/lib/mysql-files/<JID>-text-messages.tsv';
```

Video-meddelanden

```
SELECT *
FROM has_message
INNER JOIN video_message on video_message.mid = has_message.mid
LEFT JOIN products on has_message.pid = products.pid
WHERE convert(jid_str USING utf8) LIKE '%<JID>%'
INTO OUTFILE '/var/lib/mysql-files/<JID>-video-messages.tsv';
```

Deltagande JID:ar

```
select convert(jid_str USING utf8) as jid_str_utf8
from products
WHERE convert(jid_str USING utf8) LIKE '%<JID>%'
GROUP BY jid_str_utf8
INTO OUTFILE '/var/lib/mysql-files/<JID>-jids-from-all-relevant-products.tsv';
```

polisen.se

Polismyndigheten
Telefon 114 14
e-post kansli.registrator@polisen.se

Polisen

Letterhead Memorandum (Rev. 02-05-15) **EJ SEKRETESSBELAGT//REL TO USA, SWE**

USA:s Justitiedepartement (United States Department of Justice)

Federal Bureau of Investigation

Spårningsnr: 198842817
Ärendenr:SD-2864529
Prioritet: Rutin
Datum: 9 december 2021

Office of the Legal Attaché
United States Embassy
Dag Hammarskjolds Vag 31
SE-115 89, Stockholm

Nationella Operativa Avdelningen
Sektionen för internationellt polissamarbete
P.O. Box 12256
SE-102 26, Stockholm

TILL: Sambandsman

(U) SÅVIDA INTE ANNAT ANGES ELLER I EN SÄRSKILD SKRIVELSE UTTRYCKLIGEN AV HUVUDKVARTERET FÖR FEDERAL BUREAU OF INVESTIGATION (FBI)MEDGES, ÄR UPPGIFTERNA I DETTA DOKUMENT ENDAST AVSEDDA ATT ANVÄNDAS I UNDERRÄTTELSE- OCH SPÅRSYFTE, OCH ERA MYNDIGHETER FÅR INTE ANVÄNDA DESSA UPPGIFTER I DOMSTOLSFÖRFARANDEN, SPRIDA UPPGIFTERNA TILL MYNDIGHETER, PERSONER ELLER ENHETER I ANDRA STATER, ELLER VIDTA ÖPPNA UTREDNINGSÅTGÄRDER (INBEGRIPET MEN INTE BEGRÄNSAT TILL FORMELLA RÄTTSLIGA PROCESSER ELLER DIREKTKONTAKT MED DE PERSONER/ENHETER ELLER DERAS MEDHJÄLPARE DET HÄNVISAS TILL) PÅ GRUNDVAL AV UPPGIFTERNA I DETTA DOKUMENT.

(U//REL TO USA, SWE) Lämna kompletterande upplysningar rörande den rättsliga myndighet som använts i samband med Trojan Shield-utredningen.

(U//REL TO USA, SWE) Oaktat ovan angivna förbehåll, får uppgifterna i detta dokument användas i underrättelsesyfte, brottsbekämpande åtgärder, eller i rättsliga förfaranden. Uppgifterna som anges i detta dokument får i tillämpliga fall spridas till andra myndigheter i ert land, men de får inte spridas till tredjelands myndigheter eller enheter utan uttryckligt tillstånd från Federal

Bureau of Investigation. Vidare, gör Federal Bureau of Investigation inte gällande att ytterligare stöd ska tillhandahållas (t.ex. kompletterande uppgifter, autentisering, bevismaterial)med kopplingar till dessa uppgifter; ni får, emellertid, använda dessa uppgifter för att begära ytterligare information eller bistånd genom FBI:s juridiske attaché i ert land.

(U//REL TO USA, SWE) Efter diskussioner med USA:s federala åklagarmyndighet (United States Attorney's Office (USAO), beskrev USAO, med följande ordalydelse, den rättsliga grunden för Trojan Shield-operationen:

(U//REL TO USA, SWE) De tekniska metoder som inom Trojan Shields-operationen tillämpades för att driva Anomplattformarna var rättsenliga enligt Amerikas förenta staters lagstiftning och de platser dit plattformarna förlagts. Det stora flertalet av de personer som använde Anom var inte amerikanska medborgare och befann sig inte i USA. Det fjärde tillägget i USA:s konstitution gäller inte för de personerna. Därtill, var det inget av de mellan utländska användare utbytta meddelanden som passerade genom USA:s infrastruktur, dessa omfattades sålunda inte av avlyssningslagen (the Wiretap Act), 18. U.S.C §§ 2510 och följande.

(U//REL TO USA, SWE) Det tredjeland som var värd för Anom-servern ligger i EU och detta tredjeland använde sig av egen rättsprocess för att erhålla ett domstolsbeslut som godkänner att meddelanden som dirigerats till servern kopieras. Tredjelandet lämnade in meddelandena till Federal Bureau of Investigation i enlighet med en begäran om ömsesidig rättslig hjälp (MLAT). Eftersom tredjelandet följde sitt lands lag, kan Förenta staterna förlita sig på de uppgifter som erhållits angående meddelanden mellan utländska användare.

Med vänliga hälsningar

Michael S. Butsch

Polisen

PM

Datum 2022-01-26

Informationsklass
Öppen

Diarienr (åberopas) A053.007/2022

Polismyndigheten
Nationellt Forensiskt Centrum
Informationstekniksektionen

I dokumentet *Teknisk information om Operation Trojan Shield* [1] finns beskrivet hur ANØM-applikationen beräknade JID utifrån enhetens IMEI. Enligt dokumentet beräknades JID utifrån enhetens IMEI fram till december 2020, därefter ändrades formatet då det skedde förändringar i operativsystemet Android.

KAP. A3 punkt 18 - Teknisk information om Operation Trojan Shield [1]
Varje användare i ANØM identifieras med en unik identifierare (användar-ID), som tekniskt kallas för en Jabber Identifier (JID). Från början hade detta användar-ID formen av 6 alfanumeriska tecken (till exempel ”aab2c3”) och det genererades automatiskt från enhetens IMEI-nummer (International Mobile Equipment Identity number).

Kapitel A3 punkt 19 - Teknisk information om Operation Trojan Shield [1]
Enhetens IMEI-nummer kombinerades med en fast uppsättning tecken (en så kallad ”saltsträng”) för att skapa ett indatavärde. Indatavärdet genomgick en hashprocess i algoritmen MD5. De sista sex tecknen i det hashvärde som genererades var enhetens användar-ID och användarens lösenord var hela hashvärdet. Processen genomfördes automatiskt av ANØM-appen som använda detta användar-ID och lösenord för automatisk autentisering mot ANØM-servrarna.

Kapitel A4 punkt 23 - Teknisk information om Operation Trojan Shield [1]
På grund av förändringar i operativsystemet Android gick det från december 2020 inte längre att använda IMEI-numret till att automatiskt generera användar-ID. Formatet på användar-ID ändrades därför så att det genererades automatiskt i portalen. […]

Nationellt Forensiskt Centrum har analyserat ANØM-applikationen och tagit fram ett verktyg i två olika versioner [2, 3] för att beräkna ett potentiellt JID utifrån ett givet IMEI. Verktygets funktion har verifierats via stickprov av kända kombinationer av JID/IMEI. NFC har ingen kunskap om det finns undantag i de enheter som tilldelats JID eller vilka enheter som har den nya respektive den gamla tilldelningen av JID.

Referens

[1] Teknisk information om Operation Trojan Shield (2021-08-31)
[2] Beräkna JID från IMEI 210921.xlsm (Tidigare versioner av Office)
[3] Beräkna JID från IMEI 211119 Office2019.xlsm

Polisen

PM

Datum
2022-01-20

Informationsklass
BS

Polismyndigheten
Nationella operativa enheten
Patrik Zanders

Promemoria gällande tidsstämplar i Anom-material

Utredning har visat att det i vissa chattslingor med meddelanden skickade under tidsperioden 2021-02-16 - 2021-02-17 har observerats att vissa meddelanden ser ut att ha en tidsförskjutning som yttrar sig på så sätt att tidsstämpel är satt cirka två timmar efter att meddelandet faktiskt skickats.

Med anledning av ovan differenser i tidstämplar i Anom-materialet har information efterfrågats av FBI i USA som klargör detta.

I svar från FBI framkommer följande:

Runt 2021-02-16 hade upptagningsservern problem med att ansluta till enhetens infrastruktur. Smärre ändringar gjordes på upptagningsservern för att lösa dessa anslutningsproblem, vilket skapade ett separat problem med den automatiska inmatningen av data på FBI:s servrar 2021-02-17. Även om inga specifika förskjutningar av tidszoner har kunnat upptäckas, gav dessa problem upphov till manuell inmatning av data, vilket potentiellt kan ha orsakat förskjutningar i tidszoner.

Orginaltext:

On approximately 2/16/2021 the interception server had troubles connecting to the device infrastructure. Minor changes were made to the interception server to fix the connection issues, which caused a separate issue with the automated ingestion of data into FBI servers on 2/17/2021. Although no specific time zone shifts can be identified, these issues resulted in the manual process of ingesting data, which could have potentially caused time zone shifts.

Polisen

PM

Datum
2022-02-10

Informationsklass
BS

Polismyndigheten
Nationella operativa avdelningen

Promemoria gällande "*last check-in*" och "*last seen*"

Under utredning har det framkommit att det finns två olika formuleringar gällande indikationen av den senaste tidpunkt en Anom-enhet varit uppkopplad mot Anom-plattformens centrala infrastruktur.
De formuleringar som använts är ”*last check-in”* respektive ”*last seen”*.
”Last check-in” och ”last seen” avser tidpunkten då enheten senast syntes av MDM-plattformen.

Frågan som uppkommit är om dessa formuleringarna har samma tekniska betydelse?

Frågan som ställts till FBI är följande: I hola iBot och MLAT-materialet så framgår *”last check-in”* och i det kompletterande MDM-materialet så framgår *”last seen”,* frågan är om dessa två betyder samma sak eller ifall *”last seen”* indikerar något annat?

Efter svar från FBI 2022-02-02 har det bekräftats att ”*last check-in*” och *”last seen”* har samma tekniska betydelse.

Polisen

PM

Polismyndigheten
Nationella operativa avdeningen

Datum
2021-11-23

Informationsklass
Ej klassad

Diarienr (åberopas)
A688.118/2021

Saknr
403

Sky ECC

Bakgrund
Belgien, Frankrike och Nederländerna med stöd av Europol och Eurojust har genomfört en samverkansoperation mot Sky ECC:s krypterade kommunikationslösning.

I början av mars 2021 fick svensk polis information om ovanstående samverkansoperation. Svensk polis erhöll informationen eftersom operationen visat att misstänkta gärningsmän använt kommunikationslösningen i samband med grov organiserad brottslighet, som mord, våld och narkotikasmuggling i Sverige.

Sverige
Senare i mars 2021 godkändes Sverige att få ta del av information som säkrats under samverkansoperationen. Den information som erhållits har enbart varit historisk data från kommunikationslösningen till skillnad mot de tidigare operationerna avseende kryptoplattformarna EncroChat och Anom.

Under samverkansoperationerna mot kryptoplattformarna EncroChat och Anom deltog svensk polis redan i samverkansoperationens aktiva fas.

Informationen avseende Sky ECC har begärts ut av åklagare via en europeisk utredningsorder (EIO) från franska judiciella myndigheter.

Nationellt forensiskt centrum – NFC

Polisen

Förkonfigurerade enheter

Sammanfattad information om enheter med applikationen SkyECC konfigurerade med Blackberry UEM

NFC Notat 2021:01

Informationstekniksektionen

Utgivare
Nationellt forensiskt centrum – NFC
581 94 Linköping
Tfn 010-562 80 20
E-post registrator.nfc@polisen.se
www.nfc.polisen.se

Produktion Informationstekniksektionen, Polismyndigheten, 2021-01-26
Upplaga Digital version

Sammanfattning

Under första halvåret av 2020 kunde Europol avlyssna den i kriminella kretsar populära kommunikationstjänsten Encrochat. I juli 2020 offentliggjorde organisationen sina fynd.

I och med avslöjandet har de kriminella fraktionerna runt om i Europa tvingats gå över till andra kommunikationstjänster.

Några av dessa tjänster använder en legal enhetshanteringstjänst som erbjuds av det kanadensiska tjänsteföretaget Blackberry. I denna rapport sammanfattas Blackberrys tjänst och kommunikationstjänsten SkyECC som kan konstateras vara en av ersättarna till Encrochat.

Innehåll

1 Inledning

1.1 Bakgrund

Smarttelefoner specifikt förkonfigurerade för säker kommunikation har varit vanligt förekommande i brottsutredningar som är kopplade till någon form av organiserad brottslighet under lång tid. Sedan tidigt 2010-tal har olika telefonmodeller och kommunikationstjänster med olika bakomliggande teknisk lösning påträffats i samband med beslag. Det som förenar dessa kommunikationstjänster är att telefonerna är konfigurerade på ett sådant sätt att de i stort sett bara kan användas för krypterad kommunikation.

Fram till 2017 var det främst telefoner av märket BlackBerry som togs i beslag i Sverige och många av telefonerna hade sitt ursprung från det nederländska företaget Ennetcom. Som kommunikationsform användes krypterad e-post där meddelandet raderades efter en förutbestämd tid. Ennetcoms servrar togs i beslag i april 2016 och senare kunde ett antal miljoner meddelanden dekrypteras [1] [2]. Liknande beslag av servrar har gjorts på tjänster som Phantom Secure [3], IronChat [4] och PGP Safe [5].

Under perioden 2017 till 2020 var det främst enheter med en variant av operativsystemet Android, vid namn Encrochat OS, som påträffades i brottsutredningar [6]. I juli 2020 gick Europol ut med en pressrelease där man informerade att man tillsammans med ett antal medlemsländer lyckats läsa av och analysera kommunikationen i Encrochat under ett antal månader [7].

Efter att Encrochat blivit kompromitterad har flera andra former av förkonfigurerade enheter påträffats i beslag. I likhet med de tidigare Blackberry-enheter som påträffats är det vanligt att dessa mobilenheter styrs av en tjänst för mobil enhetshantering som erbjuds via legala tjänsteföretag.

1.2 Syfte

Att förse Nationellt Forensiskt Centrums uppdragsgivare med en övergripande bild över hur enheter styrda med enhetshantering använts, konfigurerats och distribuerats.

1.3 Avgränsning

I denna rapport beskrivs tjänsten mobil enhetshantering i allmänhet och enheter med applikationen SkyECC i synnerhet. Hur enheterna specifikt kan användas är strikt kopplad till vilken form av tjänst som används och hur säkerhetspolicyn är konfigurerad. NFC uttalar sig om det som är observerat vilket inte utesluter annan funktionalitet.

2 Analys

Mobilenheter som är konfigurerade med en mobil enhetshanteringtjänst är styrda med hjälp av ett antal regler som utgör en säkerhetspolicy. Mobil enhetshantering är ett vanligt verktyg för IT-avdelningar inom företag och den offentliga sektorn och gör det möjligt att övervaka, hantera och säkra de anställdas mobila enheter.

Förkonfigurerade enheter som marknadsförs som SkyECC använder Blackberrys enhetshantering för att styra och kontrollera hur enheterna används, det finns även andra liknande kommunikationsapplikationer som också använder Blackberrys enhetshantering. Inom enhetshanteringen styrs vilka applikationer som ska finnas tillgängliga och användarens möjlighet att installera nya applikationer.

2.1 Begrepp

Genom att tekniken utvecklats och därtill hur anställda får åtkomst till företagsdata som exempelvis e-post och intranät så har flertalet nya begrepp tillkommit. För bättre läsbarhet av detta dokument beskrivs några av dessa begrepp nedan.

- **Android**
  Ett operativsystem med öppen källkod för bland annat smarttelefoner och surfplattor. Operativsystemet används av flera tillverkare som exempelvis Google, Samsung, Huawei och Sony.

- **Elliptic-curve cryptography (ECC)**
  Ett antal kommunikationsapplikationer använder begreppet ECC i sitt applikationsnamn, exempelvis SkyECC. Detta är ett sätt att tala om att applikationen använder en säker kryptering. ECC är ett kryptografiskt begrepp för säkert nyckelutbyte som används vid bland annat krypterad kommunikation. I dag använder de flesta kända chatt-applikationer någon form av ECC i sin konfiguration [9].

- **Förkonfigurerade enheter**
  Ett samlingsnamn som används av Polismyndigheten. Definition: ”Förkonfigurerade enheter är enheter som används av kriminella nätverk med syfte att dölja kommunikation. Enheterna har olika fabrikat och teknisk lösning.”

- **iOS**
  Ett operativsystem för mobila enheter utvecklat av Apple exklusivt för Apple-produkter.

- **Mobile Device Management (MDM)**
  Förenklat och något kortfattat kan Mobile Device Management beskrivas som de tjänster som gör det möjligt för ett företag att kontrollera hur organisationens mobila enheter får användas. Inom MDM kan enheter lokaliseras, låsas och raderas [8].

- **Unified Endpoint Management (UEM)**
  Eftersom de tekniska behoven inom företagsvärlden har blivit mer komplex har ett vidare mer omfattande begrepp manifesterats, Unified Endpoint Management (UEM). Begreppet UEM används för tjänster som gör det möjligt att styra och säkra allt från mobilenheter, surfplattor, bärbara och stationära datorer och på senare tid även IoT-enheter (Internet of Things). UEM är tänkt att hantera en mängd olika plattformar vilket ökar möjligheterna för en organisation att låsa ned hårdvara och skydda kritisk data.

2.2 Blackberry

Blackberry är ett kanadensiskt företag känt för sitt fokus på säkra produkter. De tjänster som Blackberry erbjuder används företrädesvis av organisationer i Nordamerika. En av de tjänster som Blackberry erbjuder är Blackberry UEM som beskrivs så här på deras hemsida:

> ”…[tjänsten] ger en omfattande enhets-, applikation- och innehållshantering med integrerade säkerhets och anslutningsmöjligheter och hjälper dig hantera iOS-, macOS-, Android-, Windows 10- och Blackberry 10-enheter för din organisation.”[1]

Organisationer som är i behov att administrera mobila enheter kan ansluta sig till Blackberry UEM och få tillgång till en helhetslösning. För att kunna koppla mobila enheter till enhetshanteringen behöver organisationen både följa Blackberrys krav och riktlinjer och därtill den specifika enhetsfabrikörens krav. För exempelvis Apple-enheter behöver organisationen även vara ansluten till Apples företagslösning för att enheterna ska tillåtas att använda Blackberrys tjänst.

I korthet så registreras enheten i Blackberrys system och en klient installeras på enheten. Vilka applikationer som får finnas på enheten styrs via administrationsgränssnittet i Blackberry UEM (se bild 1).

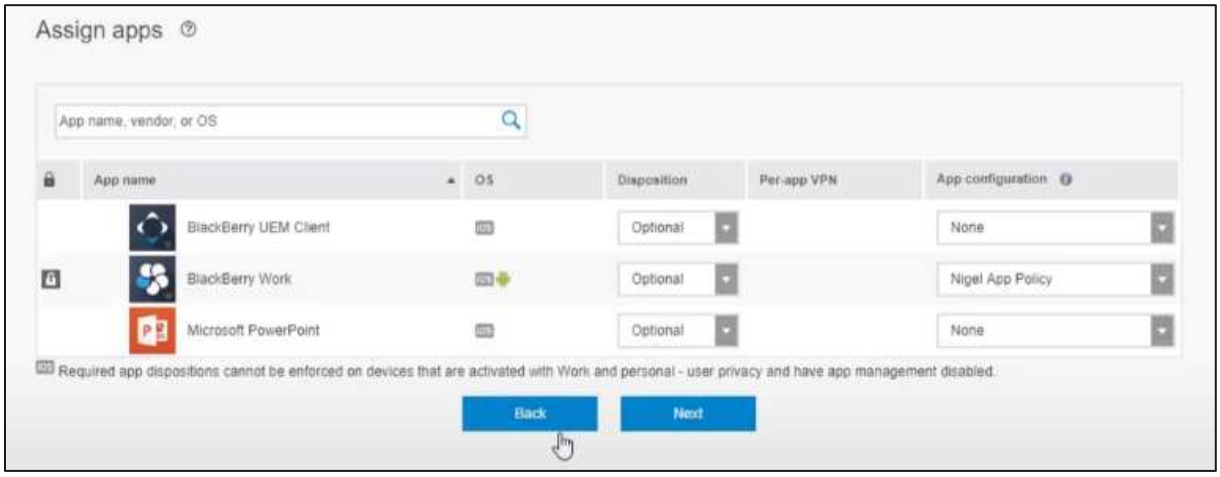


Bild 1 - Vy för att tilldela applikationer (Källa: Blackberrys användarmanual).

2.2.1 Blackberry-applikationer

Av Blackberrys applikationer har Work Apps, UEM Client samt Connectivity påträffats på enheter med SkyECC, se bild 2 för ikoner.

Bild 2 - Ikoner för Blackberrys applikationer (SkyECC).

[1] https://docs.blackberry.com/en/endpoint-management/blackberry-uem/12_13 (hämtad 2021-01-22)

Blackberry UEM App Catalog
Applikationen är namngiven som ”Work Apps” i påträffade SkyECC-enheter. Blackberry UEM App Catalog används för att granska och installera de applikationer som tilldelats användaren av Blackberry UEM-administratören. Applikationen kan likställas med Google Play eller Apple App Store.

Blackberry Connectivity
Applikationen används för att säkerställa säker kommunikation mellan organisationens nätverk och enheten.

Blackberry UEM Client
Den applikation som ser till att reglerna i säkerhetspolicyn följs.

2.3 Karaktär av ärenden

Antalet beslagtagna telefoner konfigurerade med Encrochat minskade i antal under 2020 samtidigt som antalet telefoner med SkyECC ökade i brottsutredningar av samma karaktär. Detta gör att SkyECC kan ses som en ersättare till Encrochat.

I Sverige har majoriteten av påträffade enheter med SkyECC varit av märket Apple iPhone. De ärenden där dessa telefoner påträffats har oftast varit knutna till någon form av organiserad brottslighet med brottsrubriceringar som bland annat:

- Mord eller dråp, misshandel med dödlig utgång
- Försök till mord eller dråp
- Försök, förberedelse och stämpling till mord eller dråp
- Brott mot narkotikastrafflagen
- Grovt vapenbrott

2.4 Operatör

Förkonfigurerade enheter använder vanligen endast datatrafik. Säkerhetspolicyn och det abonnemang som används hindrar användaren att ringa vanliga telefonsamtal. Vanligen har dessa enheter ett SIM-kort endast för datatrafik[2] installerat. SIM-korten är förbetalda att användas fritt under en förutbestämd tid. Abonnemangstiden varierar men 90 dagar är en vanlig tidsperiod. SIM-kort som påträffats har varit från den amerikanska teleoperatören AT&T.

2.5 Pris

Priset för förkonfigurerade enheter varierar beroende på modell, antal och tidigare kontakt med distributören. Det kan dock konstateras att priset är markant högre än att köpa en liknande telefon via vanliga inköpskanaler. Normalt brukar en förkonfigurerad telefon kosta mellan 10 000 och 20 000 SEK där abonnemangslängden vanligen är tre till sex månader. Här är det viktigt och understryka att pris och längd på abonnemang är starkt kopplat till vilken relation köparen har med distributören.

2.6 Sky Global

Verksamheten bakom applikationen SkyECC har under åren gått under namnet Sky Secure och numera Sky Global, enligt egen utsago har verksamheten sitt fäste i Vancouver, Kanada och har verkat sedan 2010. Inledningsvis erbjöd Sky Global enbart sin chattjänst på Blackberry-telefoner men under 2018 gjordes applikationen helt om. Chattklienten blev

[2] Vanligt förekommande namn är data-SIM, M2M-kort (Machine to machine) och telematikkort.

tillgänglig på operativsystemen Android och iOS, organisationen bakom applikationen kallar detta för SkyECC version 2.

Sky Global använder sig av Blackberry UEM som administratörsverktyg och applikationen SkyECC för iOS är endast tillgänglig förinstallerad på telefoner som säljs via Sky Global och dess distributörer [10]. Majoriteten av påträffade telefoner i Sverige har gått via en lokal distributör som även agerar som administratör.

Enheter konfigurerade med SkyECC är avskalade och det finns ingen möjlighet att installera andra applikationer. Det finns en telefonapplikation men vanlig telefoni är inte möjlig. De säkerhetsregler som satts upp i kombination med abonnemangstypen hos teleoperatören gör att kommunikation endast kan ske via SkyECC-applikationen.

2.7 Applikationen SkyECC

Applikationen SkyECC är en chattklient som används för att få kontakt med andra användare som har en SkyECC-telefon. Den genomgång som görs i följande kapitel är av applikationen SkyECC version 2.1. För att inloggning i applikationen ska vara möjlig behöver telefonen vara uppkopplad och ansluten till Sky Globals server. Lösenordet för att logga in (bild 3) är minst sex tecken och all information raderas efter 5 felaktiga försök. Gränsen för radering kan även ställas in på 3 eller 10 felaktiga försök. Enheterna har ett ”Emergency password” som om det skrivs in raderar all användardata i applikationen. Om inte användaren ändrar detta själv brukar standardlösenordet vara en veckodag eller en månad på engelska.

2.7.1 Inloggning

Det går att försätta applikationen i ett dolt läge, kallat ”Stealth Mode”. Med applikationen i dolt läge ändras ikonen för SkyECC till en miniräknare och när applikationen startas öppnas istället en vy som till synes ser ut som en miniräknare (bild 4). För att komma till den normala inloggningsrutan behöver användaren först slå in ett lösenord i form av ett aritmetiskt uttryck, exempelvis 45x45.

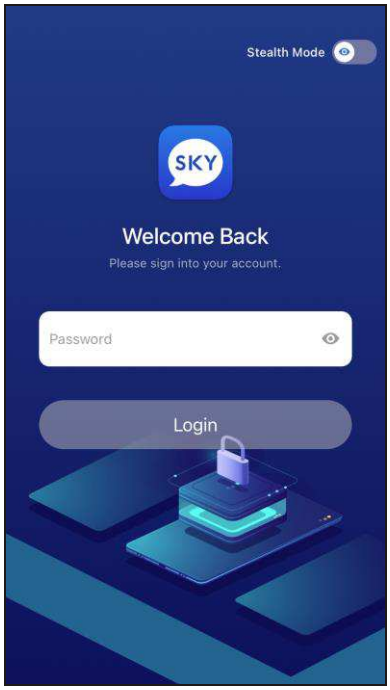


Bild 3 - Inloggningsrutan för SkyECC

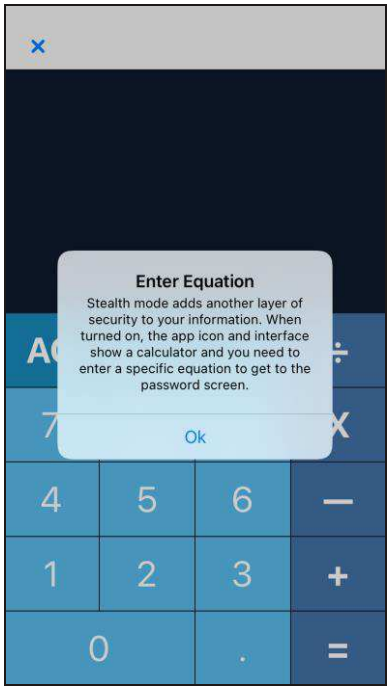


Bild 4 - SkyECC i Stealth mode

2.7.2 *Identifiering*

Till varje konto autogenereras en bild och ett namn (se bild 5). Båda dessa kan ändras av användaren och varken namn eller bild behöver vara unikt. Varje användare har också ett unikt ECC ID som innehåller sex tecken, exempelvis AB12CD. Varje användare kan även lägga till ett meddelande, ”Status Note”, som alla kontakter kan se direkt. I likhet med ”Status” i Encrochat så är det vanligt förekommande att ge information om ny tillgänglighet, exempelvis *”Hasch and coke in stock!”* eller *”Finns koks”*.

På en ny enhet finns vanligen två kontakter, ”Support” som är Sky Globals supportkonto och en administratörskontakt som är den lokala distributören (bild 6). För att initiera en ny kontakt behöver användaren ange den nya kontaktens unika ECC ID.

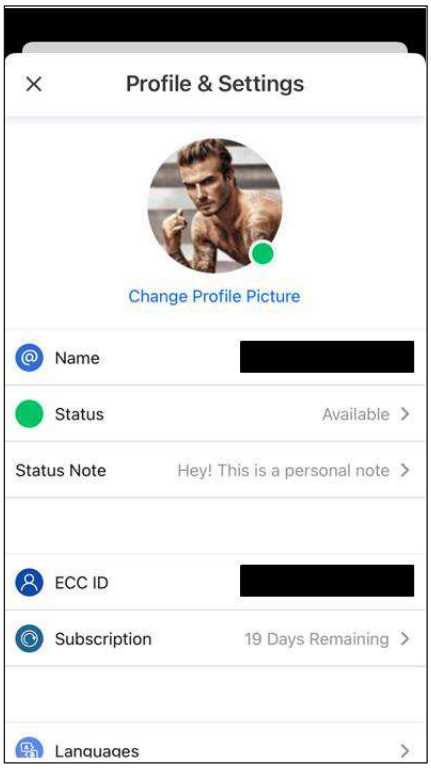


Bild 5 - Användaruppgifter

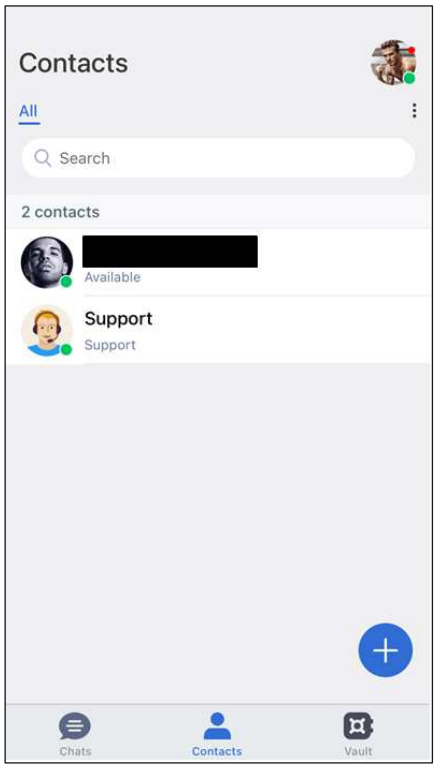


Bild 6 - Kontakter

2.7.3 *Valv*

I applikationen finns ett valv som skyddas med ytterligare ett lösenord, lösenordet måste vara minst ett tecken. I valvet går det att spara bilder, notiser och chattmeddelanden.

Bilder

Med valvet uppstartat kan bilder tas som sedan kan kategoriseras i olika album. Tagna bilder saknar platsinformation.

Noteringar

Textnotiser kan skrivas och sparas i valvet. Notisen innehåller en rubrik och en brödtext. Notiser kan kategoriseras efter kategorier.

Chattmeddelanden

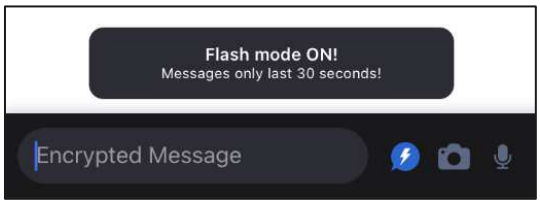
Vanligen raderas chattmeddelanden efter en förutbestämd tid, dock går det att spara meddelanden i valvet.

2.7.4 Chatt

Användaren kan skicka ett chattmeddelande till initierade kontakter och i de grupper som denne tillhör. I chattvyn finns en inmatningsruta (bild 7). De olika typer av meddelande som kan skickas finns förklarade i Tabell 1. Alla meddelanden är antingen högerställda (skickade meddelanden) eller vänsterställda (mottagna meddelanden), dessa visualiseras i bild 8.

Bild 7 - Inmatning av meddelanden

Tabell 1 - Teckenförklaring av olika typer av meddelanden. Numrering från bild 7

1	Bifogade bilder, notiser och chattar som är sparade i applikationens valv (se föregående avsnitt). Därtill går det att vidarebefordra en kontakt.
2	Textmeddelanden  Bild 8 - Skickade respektive mottagna meddelanden
3	”Flash-meddelande”. Det innebär att meddelandet raderas 30 sekunder efter att de har lästs.  Bild 9 - Inmatning av meddelanden i "Flash Mode"
4	Bilder tagna med telefonens kamera.
5	Ljudmeddelanden som kan spelas in i realtid. Mottagaren behöver sedan klicka på meddelandet för att spela upp ljudinspelningen.  Bild 10 - Inspelat ljudmeddelande med en längd på fem sekunder

2.7.5 Broadcast

Det går att sända ut ett meddelande till alla kontakter samtidigt vilket görs via ett så kallat ”broadcast message”.

2.7.6 Grupper

Den användare som skapar en gruppchatt blir automatiskt ägare och administratör. Ägaren kan sedan lägga till andra gruppmedlemmar som administratörer. En administratör kan endast lägga till kontakter som redan har initierats individuellt. De tester som utförts talar för att individuella gruppmedlemmar inte behöver ha initierat kontakt med övriga i gruppen.

3 Slutsats

- SkyECC är en applikation för säker kommunikation av text, ljud och bild. Applikationen finns på mobila enheter som styrs via en enhetshanteringstjänst från Blackberry.

- Det kan konstateras att enheter med SkyECC endast har en applikation som användaren kan använda. Det går inte att använda enheterna till någon annan form av kommunikation.

- Mobila enheter för privatpersoner som styrs via Blackberry UEM är en ovanlig företeelse i Sverige och Europa. De flesta enheter som har påträffats i Sverige har varit i samband med brottsutredningar kopplade till organiserad brottslighet.

- Enheter styrs och konfigureras av Sky Global, en extern organisation, alternativt via en lokal administratör. Telefonerna har ett förhållandevis högt pris och kort abonnemangsperiod.

4 Källor

[1] Paganini, P., Security Affairs (2017-03-10). The Dutch police decrypted a number of PGP messages sent by crooks through their BlackBerry mobile devices for the criminal investigation on Ennetcom. https://securityaffairs.co/wordpress/57036/cyber-crime/blackberry-pgp-messages [Hämtad 2020-09-08]. **Internetreferens**

[2] Cox. J., Vice (2017-03-09). Dutch Cops Say They've Decrypted PGP Messages On Seized Server. https://www.vice.com/en_us/article/3dyaqk/dutch-cops-say-theyve-decrypted-pgp-messages-on-seized-server [Hämtad 2020-09-08]. **Internetreferens**

[3] Federal Bureau of Investigation. International Criminal Communication Service Dismantled (2018-03-16). https://www.fbi.gov/news/stories/phantom-secure-takedown-031618. [Hämtad 2020-09-15]. **Internetreferens**

[4] Vaas. L., Naked Security. 258,000 encrypted IronChat phone messages cracked by police (2018-11-09). https://nakedsecurity.sophos.com/2018/11/09/258000-encrypted-ironchat-phone-messages-cracked-by-police. [Hämtad 2020-09-15]. **Internetreferens**

[5] Khandelwal. S., The Hacker News. Dutch Police Seize Another Company that Sells PGP-Encrypted Blackberry Phones (2017-05-11). https://thehackernews.com/2017/05/police-blackberry-pgp-phones.html. [Hämtad 2020-09-15]. **Internetreferens**

[6] Nationellt Forensiskt Centrum. Förkonfigurerade enheter – Sammanfattad information om Encrochat OS. NFC Notat, Informationstekniksektionen 2020:09. **Interna rapporter & Notat**

[7] Europol. Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe (2020-07-02). https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe. [Hämtad 2020-12-23]. **Internetreferens**

[8] Cheuvront, D., Security Intelligence. Why UEM Is the New MDM: The Latest Stage in Enterprise Evolution (2018-07-03). https://securityintelligence.com/why-uem-is-the-new-mdm-the-latest-stage-in-enterprise-evolution. [Hämtad 2020-12-23]. **Internetreferens**

[9] Secure Messaging Apps Comparison (2021-01-19). https://www.securemessagingapps.com/ [Hämtad 2021-01-22]. **Internetreferens**

[10] SKY ECC User Guide for Android and iOS (maj 2019). https://www.skyecc.com/wp-content/uploads/2019/05/SKY-App-User-Guide-expanded-with-iOS.pdf [Hämtad 2020-01-22]. **Användarmanual**

nfc.polisen.se

Nationellt forensiskt centrum – NFC
581 94 Linköping, Telefon 010-562 80 20
e-post registrator.nfc@polisen.se

Swedish National Forensic Centre – NFC
SE-581 94 Linköping, Tel +46 10 562 80 20
e-mail registrator.nfc@polisen.se

Polisen

Polisen

PM

Datum
2022-01-21

Informationsklass
Ej klassad

Diarienr (åberopas)

Polismyndigheten
Nationella Operativa Avdelningen

PM gällande koppling mellan Sky PIN och IMEI

Informationen i detta PM utgår ifrån information som Polismyndigheten har vid dagens datum 2022-01-21.

I exportsvar på begäran som ställs via en EIO till Frankrike så mottar utredningar i Sverige Sky-material för förundersökning där en till flera IMEI-nummer kan anges som kopplade till en viss Sky-PIN. I skrivande stund (2022-01-21) har Sverige ännu inte fått ett svar från Frankrike som förklarar vad en länkning mellan IMEI och PIN innebär, vad källan till dessa länkningar är samt vilken tidsperiod som varje länkning avser.
Det är i skrivande stund även oklart om Frankrike någonsin kommer att kunna ge ett konkret svar på kopplingen IMEI och PIN.

Det finns meddelanden och konversationer i Sky-materialet som tyder på att det är möjligt att flytta en Sky-PIN mellan olika SIM-kort och telefoner. Dessa flyttar verkar utföras av särskilda administratörer.

Polisen

PM

Datum
2021-11-09

Informationsklass
Öppen information

Polismyndigheten
Nationellt Forensiskt Centrum

Diarienummer:
A661.881/2021

Tolkning av information i extraheringsrapport för SkyECC

Dokumentation för funktionaliteten för chattapplikationen SkyECC finns inte tillgänglig publikt. Applikationsdata på mobilenheter finns oftast sparad i databaser som innehåller en stor mängd data. Viss data i databasen inte är presentabel eller relevant för en människa. Vid analys av en extrahering tolkas data till information. Detta PM beskriver hur viss extraherad data från applikationen SkyECC tolkats. Samma data kan ha inhämtats av annan aktör på annat sätt och tolkningen kan då skilja sig.

Teknisk tolkning av data

När data från en okänd applikation analyserats utförs om möjligt forensiska tester för att förstå och tolka data. Därtill görs vissa antaganden av vad viss data kan betyda. Antaganden görs utifrån kunskap hur chattapplikationer generellt fungerar.

Ett exempel på antagande gäller fältet `is_out` som existerar för varje meddelande i databasen för SkyECC-applikationen Fältet har antingen värdet 1 eller 0. I tabell 1 presenteras den tolkning NFC har gjort.

Tabell 1 - Tolkning av fältet is_out i databasen

Fält	Exempel på värde	Tolkat som
`is_out`	1	Skickat meddelande
`is_out`	0	Mottaget meddelande

Flera meddelande-id

Vissa fält är inte uppenbart namnsatta och därmed är det svårare att tolka och förstå hur denna har data genererats. Ett exempel är fältet `id` i databasen som NFC tolkat som ett meddelande-id.

Värdet är ett unikt heltal som tilldelats varje meddelande i databasen. Om en fil bifogas i ett meddelande märks den bifogade filen med detta heltal. Fältet finns presenterat i den extraheringsrapport som har genererats vid analys av en SkyECC-databas[1]. Värdet id är att beteckna som unikt för telefonen men ska inte tolkas som kronologiskt.

[1] Rapporter genererade från och med juni 2020.

Exempel:
1. Användaren börjar skriva på ett utgående meddelande 2021-11-01 10:45, meddelandet får id 1.
2. Ett nytt meddelande tas emot 2021-11-01 10:47. Detta meddelande får id 2.
3. Användaren skriver klart sitt utgående meddelande och skickar det 2021-11-01 10:50.

Med ovanstående scenario kan det se ut enligt Tabell 2 i databasen.

Tabell 2 - Tolkning av id kontra tid

id	Typ	Tidsstämpel
2	Mottaget meddelande	2021-11-01 10:47
1	Skickat meddelande	2021-11-01 10:50

Skillnad i tidsstämplar

För en viss version av applikationen SkyECC sparades meddelanden i två olika filer på enheten. Dels i applikationens databas samt i en separat loggfil. NFC har ingen kännedom om funktionen bakom eller syftet med meddelanden som sparas i loggfilen. I de rapporter som genererats av NFC rubriceras meddelanden som hämtats från databasen för ’Meddelanden per kontakt’ och meddelanden som hämtas från loggfilen presenteras under rubriken ’Meddelanden från logg’.

Det NFC kan konstateras är att tidsstämplarna är olika. Det kan antas att tidsstämpeln som varje meddelande får är baserat på tidpunkten när meddelandet sparas i respektive fil.

Meddelanden i loggen tycks sparas gruppvis och flera meddelanden kan då få samma tid. Tiden för meddelanden under ’Meddelanden från logg’ ska därför ses som ungefärlig och inte exakt.

Då tidsstämplarna i loggen sparas gruppvis är bedömningen att tidsstämplar under ’Meddelanden per kontakt’ är mer tillförlitlig än tidsstämplar under ’Meddelanden från logg’.

Pressmeddelande från Eurojust gällande Sky ECC

Rättsliga och brottsbekämpande myndigheter i Belgien, Frankrike och Nederländerna har i nära samarbete vidtagit kraftfulla åtgärder för att förhindra brottsnätverks användning krypterad kommunikation. Åtgärderna har vidtagits med stöd från Europol och Eurojust. Genom kontinuerlig övervakning av brottslig användning av kommunikationstjänsten Sky ECC har utredare i de tre inblandade länderna fått direkt insyn i flera hundra miljoner meddelanden som skickats mellan kriminella. På så sätt har man kunnat samla in avgörande information om fler än hundra fall av storskalig brottslig verksamhet och därmed förhindrat potentiellt livshotande situationer.

Under en insatsdag den 9 mars 2021 genomfördes ett stort antal gripanden och en mängd husrannsakningar och beslag i Belgien och Nederländerna. Operationen är en viktig del av rättsliga och brottsbekämpande myndigheters ständiga arbete, såväl inom som utanför EU, med att förhindra olaglig användning av krypterad kommunikation, vilket även visades förra året med den framgångsrika avkrypteringen av kommunikationsplattformen EncroChat.

Från mitten av februari kunde myndigheterna följa ungefär 70 000 Sky ECC-användares informationsflöden. Många EncroChat-användare bytte till den populära plattformen Sky ECC efter att EncroChat knäcktes 2020.

Den information som har inhämtats efter att Sky ECC avkrypterades kommer att ge värdefulla insikter om brottslig verksamhet i flera EU-medlemsländer och tredje länder, och den kommer att bidra till utökade utredningar och till att lösa grova och gränsöverskridande brott i många månader framöver, kanske till och med flera år.

Under den senaste månaden har brottsbekämpande myndigheter i alla tre länderna stått beredda att snabbt reagera på farlig brottslig verksamhet, om det behövs. Den inhämtade informationen kommer nu att analyseras ingående.

Utredningen av verktyget inleddes i Belgien efter att mobiltelefoner som beslagtagits i utredningar visade att Sky ECC användes. I hela världen använder ungefär 170 000 individer verktyget, som har sin egen infrastruktur och egna applikationer. Verktyget drivs från USA och Kanada men med servrar baserade i Europa. På global nivå skickas omkring tre miljoner meddelanden om dagen med Sky ECC. Över 20 procent av användarna är baserade i Belgien och Nederländerna.

Europol har bidragit, och kommer att fortsätta bidra, med taktiskt, tekniskt och ekonomiskt stöd till Belgien, Nederländerna och andra inblandade länder. Europol kommer också att analysera detta viktiga informationsflöde för att stoppa livshotande situationer och allvarlig brottslighet.

Källa: https://www.eurojust.europa.eu/new-major-interventions-block-encrypted-communications-criminal-networks
Publiceringsdatum: 2021-03-10

Eurojust har gett råd och stöd om gränsöverskridande rättsligt samarbete och organiserat tolv samordningsmöten för att möjliggöra samarbetet. Eurojust kommer att fortsätta ge sådant stöd och är redo att tillhandahålla ytterligare rådgivning och gränsöverskridande operationellt ekonomiskt stöd till alla inblandade medlemsstater och länder för att säkerställa ett väl fungerande gränsöverskridande rättsligt samarbete.

Följande myndigheter deltog i operationen:

Belgien: Federala åklagarkontoret, Åklagarkontoret i Antwerpen, Undersökningsdomstolen i Mechelen, Federala kriminalpolisen, Federala polisen och DSU-enheten
Frankrike: Nationella jurisdiktionen mot organiserad brottslighet (JUNALCO), Kriminalpolisens centraldirektorat (DCPJ)
Nederländerna: Nationella åklagarbyrån, Åklagarkontoret i Amsterdam, Nationella polisen
Relaterade taggar: Organised crime, Europol, Belgium, France, Netherlands

Källa: https://www.eurojust.europa.eu/new-major-interventions-block-encrypted-communications-criminal-networks
Publiceringsdatum: 2021-03-10

Polisen

NFC IT Notat 2020-09
Förkonfigurerade enheter

Signerat av

Signerat datum

Enhet
Region Mitt, Aktionsgrupp 1 Rgn Mitt

Diarienr
5000-K355469-21

Orginalhandlingens förvaringsplats

Datum
2021-04-15

Tid
08:41

Involverad personal	Funktion
Johan Ericson	Uppgiftslämnare

Nationellt forensiskt centrum – NFC

Polisen

Förkonfigurerade enheter

Sammanfattad information om Encrochat OS

NFC Notat 2020:09

Informationstekniksektionen Roland Andersson, Tommy Färnqvist

Utgivare
Nationellt forensiskt centrum – NFC
581 94 Linköping
Tfn 010-562 80 20
E-post registrator.nfc@polisen.se
www.nfc.polisen.se

Produktion Informationstekniksektionen, Polismyndigheten, 2020-09-18
Upplaga Digital version

Sammanfattning

Enheter med Encrochat konfigurerat började synas i brottsutredningar under 2017 och har under de tre efterföljande åren varit en mycket populär kommunikationstjänst för individer som verkar inom organiserad brottslighet runt om i hela Europa. Telefonerna är avskalade i funktionalitet och det går inte att installera egna applikationer, kommunikation kan endast ske med en annan användare som har en Encrochat-telefon.

Innehåll

1 Inledning

1.1 Bakgrund

Smarttelefoner specifikt förkonfigurerade för säker kommunikation har varit vanligt förekommande i brottsutredningar som är kopplade till någon form av organiserad brottslighet under lång tid. Under hela 2010-talet har olika telefonmodeller och kommunikationstjänster påträffats i samband med beslag. Den bakomliggande tekniska lösningen varierar men det som förenar dessa kommunikationstjänster är att telefonerna är konfigurerade på ett sådant sätt att de i stort sett bara kan användas för krypterad kommunikation.

Fram till 2017 var det främst telefoner av märket BlackBerry som togs i beslag i Sverige där många av telefonerna såldes av det nederländska företaget Ennetcom. Som kommunikationsform användes krypterad e-post där meddelandet raderades efter en förutbestämd tid. Ennetcoms servrar togs i beslag i april 2016 och senare kunde ett antal miljoner meddelanden dekrypteras [1] [2]. Liknande beslag av servrar har gjorts på tjänster som Phantom Secure [3], IronChat [4] och PGP Safe [5].

Genom beslagen av servrar minskade BlackBerry i popularitet och telefoner konfigurerade med Encrochat OS började tas i beslag under 2017. Fram till våren 2020 då det framkom att tjänsten blivit komprometterad har det varit en populär kommunikationstjänst inom kriminella nätverk över hela Europa.

1.2 Syfte

Att förse Nationellt Forensiskt Centrums uppdragsgivare med en övergripande bild över hur kommunikationstjänsten Encrochat OS har använts, konfigurerats och distribuerats. Detta är en komplettering av NFC IT Notat 2018:04 och riktar sig främst till funktionen på telefonmodellerna BQ Aquaris X2, BQ Suro Carbon samt Vsmart.

1.3 Avgränsning

I denna rapport beskrivs en tjänst bestående av en modifierad och odokumenterad variant av operativsystemet Android samt tillhörande applikationer för säker kommunikation. Det är viktigt att påtala att det har funnits olika versioner av Encrochat OS som är avsedda för olika telefonmodeller. NFC uttalar sig om det som är observerat vilket inte utesluter annan funktionalitet.

2 Introduktion

Verksamheten bakom Encrochat har skapat två operativsystem baserade på Android. Ett säkert system som fått namnet *Encrochat OS* och ett öppet system som av upphovsinnehavarna har döpts till *Android OS*. I detta dokument särskiljs telefonmodellen BQ Suro Carbon från övriga modeller då funktionen skiljer sig så pass mycket.

2.1 Kort beskrivning av Android

Android är en plattform med öppen källkod[1] och är ett Linux-baserat operativsystem för bland annat smarttelefoner och surfplattor. För att få använda varumärket Android och programbiblioteket[2] Google Play måste vissa kompatibilitetskrav uppsatta av Google följas. Stora telefontillverkare som Samsung och Sony följer dessa krav och skapar sin egen variant av Android. Det finns också andra egentillverkade varianter av Android som inte använder varumärket. De egentillverkade operativsystemen är fullt legala och utformas med exempelvis användarvänlighet eller säkerhet i fokus.

Encrochat OS är ett egentillverkat Android-system där många standardfunktioner är borttagna. Det finns inget programbibliotek så användaren kan bara använda de applikationer som finns installerade och möjligheten att ändra inställningar är mycket begränsat.

2.2 Telefonfabrikat

De telefonmodeller som konfigurerats med Encrochat OS är relativt billiga Android-telefoner och är troligen utvalda för att det är lätt att installera en modifierad variant av Android på dessa enheter. Telefoner från tre telefontillverkare har påträffats i Sverige – OnePlus (Kina), BQ (Spanien) och VSmart (Vietnam). Påträffade modeller i kronologisk ordning nedan.

- OnePlus 3
- OnePlus X
- BQ Aquaris X5 Plus
- BQ Aquaris X
- BQ Aquaris X2
- Vsmart
- BQ Aquaris Suro Carbon

VinGroup, företaget bakom Vsmart, köpte under 2018 upp majoriteten av aktierna i BQ. I samband med överenskommelsen åtog sig BQ att producera de första Vsmart-telefonerna [6]. Vsmart-modeller med Encrochat OS som påträffats är i jämförbara med BQ Aquaris X2.

2.3 Inköp

Förkonfigurerade telefoner har ett förhållandevis högt pris. Priset för Ennetcoms BlackBerry-telefoner låg under 2016 på cirka 1500 euro [1]. De telefonmodeller som Encrochat har använt sig av kostar 300 – 400 euro via vanliga inköpskanaler, med Encrochat OS installerat har priset varit någonstans mellan 1000 – 2000 euro beroende på modell och inköpskanal.

De första Encrochat-telefonerna som lanserades kunde köpas in via olika marknadsplatser som exempelvis Ebay. Under åren har verksamheten bakom blivit mer ljusskygg vilket gjort att inköpen sker via personlig kontakt eller via de kontakter som funnits på Encrochats olika hemsidor[3].

[1] Programkod som är publikt tillgänglig. Vem som helst kan få tillgång till, ändra och distribuera koden på valfritt sätt.
[2] I detta dokument menas en webbaserad butik för att installera applikationer på enheten.
[3] Många av Encrochats hemsidor har stängts ned vid detta dokuments uppförande.

2.4 Operatör

Telefonerna levererades med internationella SIM-kort[4] förbetalda för fri dataanvändning under en bestämd tid, vanligen 3, 6 eller 12 månader. Majoriteten av påträffade SIM-kort har varit av typen data-SIM[5], det är inte möjligt att använda ett data-SIM för att ringa vanliga telefonsamtal. Större dele n av de SIM-kort som påträffats i Sverige har varit från den nederländska operatören KPN men också enstaka SIM-kort från Tele2 och Telenor har observerats.

2.5 Identifikation

En mobilenhet kan erbjuda möjligheten att två SIM-kort kan användas och då har enheten tilldelats två IMEI-nummer[6]. På Android går det att gå in under inställningar för att se enhetens IMEI-nummer. I de Encrochat-telefoner som har analyserats stämmer inte IMEI-numren överens mellan Android OS och Encrochat OS. NFC kan inte säga något med bestämdhet om de IMEI-nummer som finns i systemen eller hur de används då variationen är för stor.

Enhetens faktiska IMEI-nummer går vanligen att hitta på en etikett inuti enheten. På modellerna BQ Aquaris X2 och VSMART kan de faktiska IMEI-numren på enheten avläsas genom att avlägsna bakstycket, se bild 3.

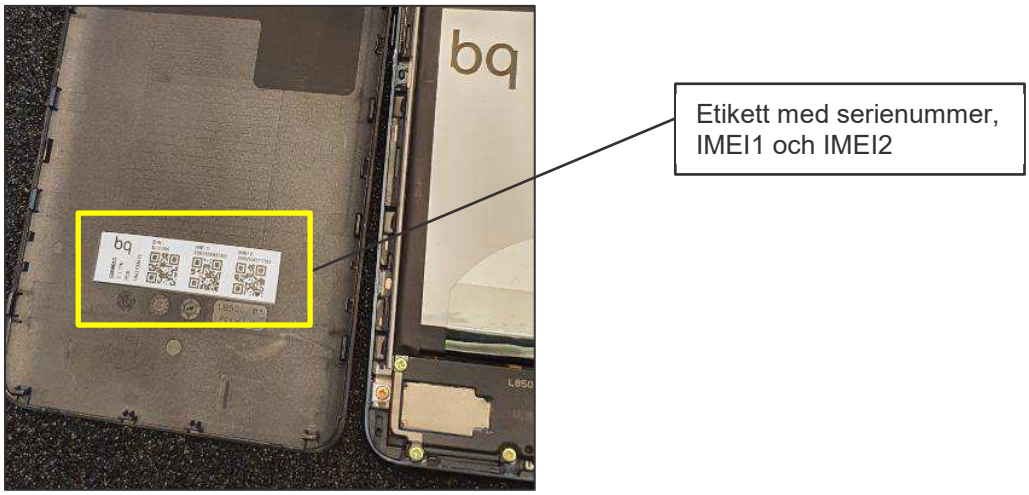


Bild 1 – Insidan av bakstycke på BQ Aquaris X2

2.6 Android OS

Android OS är det operativsystem som startar på Encrochat-telefoner med ett tryck på strömknappen. Syftet med systemet är främst för att dölja det faktum att det är en Encrochat-telefon. Under de tre år som dessa enheter påträffats i beslag har Polismyndigheten inte funnit några indikationer på att Android OS har haft någon större funktionell betydelse.

2.6.1 Lösenordsskydd

På ett fåtal enheter har användaren satt ett lösenord på Android OS men på de flesta beslagtagna enheter startar Android OS utan lösenord. På BQ Suro Carbon har användaren möjlighet att förse Android OS med ett lösenord och ett annat för Encrochat OS. Beroende på vilket lösenord som skrivs in startar respektive system.

---

[4] Telefonnumret och abonnemanget är knutna till SIM-kortet. Varje SIM-kort har ett unikt id så kallat IMSI.
[5] SIM-kort för endast data och inte traditionella telefonsamtal. Tekniken kallas m2m (machine-to-machine).
[6] Alla mobiler har minst ett unikt, 15-siffrigt så kallat IMEI-nummer. Det används för att identifiera enskilda mobiltelefoner i mobilnätet.

2.6.2 Applikationer

De applikationer som finns för kommunikation är oanvändbara då kontakt med omvärlden är avstängd i Android OS. Det går inte att aktivera trådlöst nätverk eller ringa vanliga samtal med telefonapplikationen. På BQ Suro Carbon finns däremot möjlighet att använda två SIM-kort. Det andra SIM-kortet kan vara ett traditionellt SIM-kort som ger möjlighet att ringa vanliga samtal. På BQ Suro Carbon går det även att ansluta till ett trådlöst nätverk.

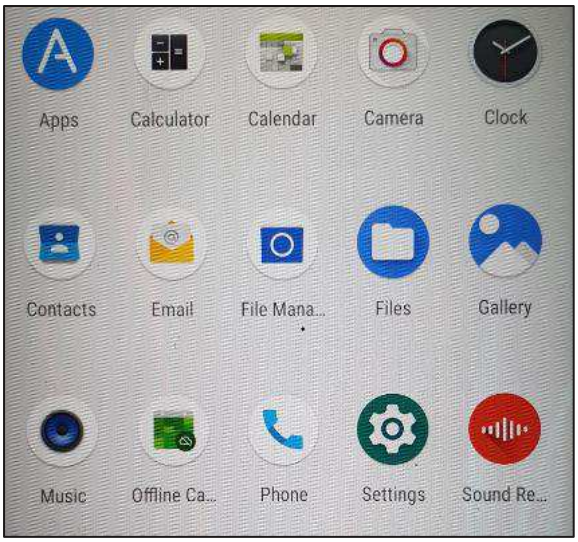


Bild 2 – Applikationer i Android OS på BQ Suro Carbon

Bild 3 – Applikationer i Android OS på BQ Aquaris X2

2.7 Encrochat OS

Det lösenordsskyddade systemet har döpts till Encrochat OS. Systemet startas via en viss knappkombination som varierar beroende på telefonmodell. Exempelvis på de tidigaste telefonmodellerna startas Encrochat OS genom att användaren med telefonen avstängd trycker in strömknappen samtidigt som en av volymknapparna.

2.7.1 Lösenordsnivåer

Encrochat OS är lösenordsskyddad med flera lösenord. När enheten startar upp skyddas systemet av ett så kallat disklösenord. Disklösenordet måste innehålla minst 15 alfanumeriska[7] tecken. De enheter som observerats har funktionen ”*Shutdown after inactivity’* aktiverat. Inställningen innebär att om enheten inte används inom en 24-timmarsperiod efter senaste upplåsningen så stängs enheten av, då måste disklösenordet skrivas in återigen.

Nästa nivå av säkerhet är ett skärmlösenord som måste vara minst 6 alfanumeriska tecken. Är enheten inaktiv för länge så behöver skärmlösenordet skrivas in återigen. Genom en viss sifferkombination kallat ”Panic PIN” kan allt på enheten raderas, sifferkombinationen måste vara minst en siffra. Slutligen skyddas applikationen Notes med en lösenordsfras.

2.7.2 Språk

Som standardspråk används *English (United States)*, det går att ställa in andra språk som svenska. Då Encrochat OS är ett egentillverkat operativsystem är dock inte alla menyer översatta. Språkinställningen har inget att göra med funktionen i övrigt eller med tidsinställningen på enheten.

[7] En teckenuppsättning som innehåller både siffror 0–9, bokstäver A–Ö och eventuellt inkluderande skiljetecken och andra specialtecken

2.7.3 Tid och tidszon

Encrochat OS använder de tidsfunktioner som finns som standard i Android. Inställningarna *”Automatiskt datum och tid”* samt *”Automatisk tidzon”* är som standard aktiverat och innebär att tiden hämtas från mobilnätet och klockan uppdateras med den lokala tiden. Denna inställning går att stänga av och manuell tid går att ställa in (gäller alla Android-enheter och inte bara Encrochat-telefoner).

2.7.4 Positionsdata

På de telefoner som har observerats har inställningen platstjänster[8] inaktiverats eller helt plockats bort vilket har till följd att enheterna inte kan platsbestämmas. Det avtryck som enheterna lämnar är kontakten med mobilnätet och närmaste basstation. Denna information och dess precision är inte synbar i enheterna och är inget NFC har möjlighet att uttala sig om.

2.7.5 Applikationer

Encrochat OS innehåller ett bestämt antal applikationer, det går inte att installera nya. På de enheter som påträffats finns ingen vanlig telefonapplikation vilket omöjliggör vanliga telefonsamtal. En jämförelse mellan applikationerna på två telefonmodeller kan ses i Bild 4 och Bild 5. Tre applikationer är centrala i operativsystemet och det är Chat, Note och Status och fram till 2018 fanns även en applikation för e-post vid namn EncroMail/EncroPGP som har försvunnit i senare versioner av Encrochat.

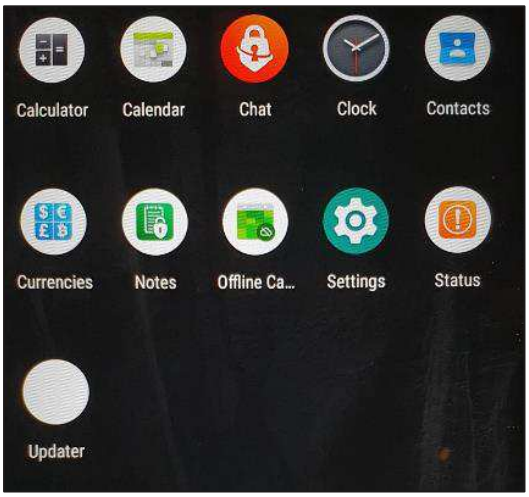


Bild 4 - Applikationer i Encrochat OS på BQ Suro Carbon

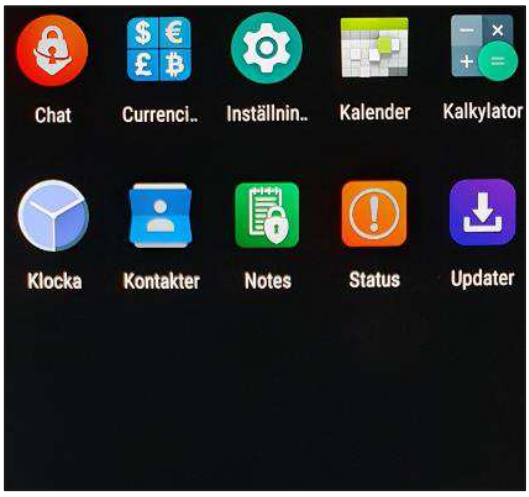


Bild 5 - Applikationer i Encrochat OS på BQ Aquaris X2

[8] Med platstjänster aktiverat samlar enheten in data via GPS, Bluetooth, wifi och mobilmaster för att fastställa ungefärlig plats.

Applikationen Status

Applikationen ger information om det abonnemang som telefonen är knuten till gentemot Encrochat, se bild 6. Antalet dagar som Encrochat-abonnemanget är aktivt varierar.

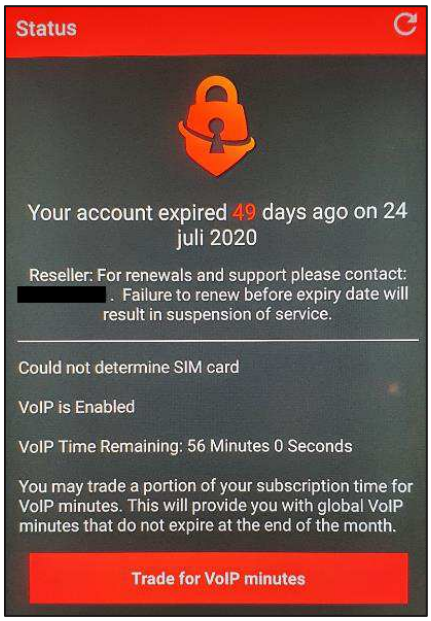


Bild 6 - Applikationen Status (maskerat reseller-användarnamn)

Applikationen Notes

Applikationen Notes skyddas av en lösenordsfras, 15 alfanumeriska tecken är rekommenderat men ett lösenord på ett tecken godkänns. Noteringarna sparas med datum enligt Bild 7. En notering innehåller en rubrik och en löptext (Bild 8), på de enheter som observerats kan noteringar endast innehålla text. Texten kan kopieras till urklipp för att sedan klistras in i en annan notering eller i ett meddelande.

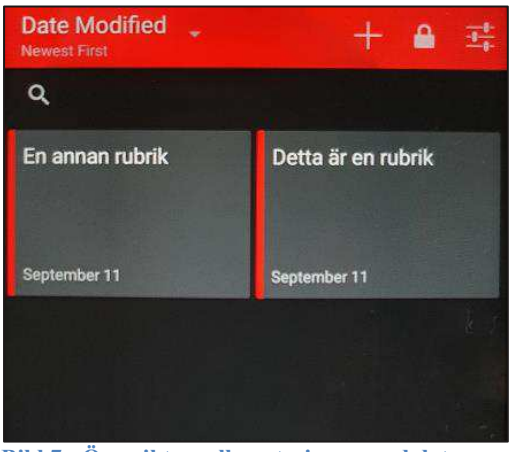


Bild 7 - Översikt av alla noteringar med datum

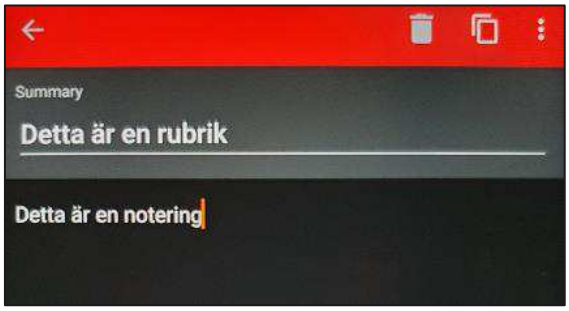


Bild 8 - En notering

Applikationen Chat
Applikationen Chat är den centrala delen i Encrochat OS och som operativsystemet fått sitt namn ifrån. Kommunikation kan ske via text, bild och tal med vissa variationer mellan olika telefonmodeller.

Gruppchatt
NFC har inte funnit några indikationer på att gruppchatt har varit möjlig. Det finns tecken på att verksamheten bakom Encrochat har haft som mål att erbjuda sådan funktionalitet i framtiden. Det kan finnas så kallade utvecklarkonton där denna funktionalitet kan ha testas men inte till den stora massan.

Status
Användaren kan sätta en egen status som kan ses av alla kontakter, exempel på status som observerats är ”*Amfetamin in*” och ”*Top coca, hash, weed & speed in!*”.

Användarnamn (Username)
Varje användare i chatt-nätverket identifieras via ett användarnamn som är unikt. I de flesta fall är användarnamnet förvalt när telefonen levereras och består vanligen av två engelska ord, till exempel *reel* och *cub*. Även egenvalda användarnamn har observerats vilket troligen är en överenskommelse mellan Encrochat och extra speciella användare.

Det mesta tyder på att användarnamnet inte går att flytta mellan två telefoner då det finns exempel på användare som valt ett användarnamn som varit snarlikt ett de tidigare använt. I samband med att vissa användare har uppgraderat sitt abonnemang och bytt från en äldre BQ Aquaris X2 till en BQ Suro Carbon har det funnits möjlighet att flytta sitt konto till den nya telefonen.

Smeknamn (Nickname)
Användaren kan sätta ett smeknamn på en befintlig kontakt. NFC har inte funnit några tecken på att smeknamnet används mer än lokalt på telefonen.

Kontakter
För att lägga till en ny kontakt skapas en inbjudan (eng. invite) där kontaktens användarnamn behöver anges tillsammans med ett meddelande till den man vill bjuda in. Om motparten godkänner inbjudan skapas en kontakt. Bild 9 visar en kontaktsida, där kontaktens namn finns längst upp till vänster (maskerat), bredvid syns ikonen för röstsamtal som sker via tekniken internettelefoni[9].

Meddelanden är vänster- respektive högerställda beroende på om meddelandet är skickat eller mottaget, på Bild 9 syns endast vänsterställda meddelanden. Bredvid meddelandedatumet anges livslängden på meddelandet tillsammans med en brandlåga.

Längst ned på kontaktsidan sker inmatningen av meddelandet, ikonerna bredvid meddelandet har följande betydelse.


Används för att ställa in livslängden på meddelandet i antalet dagar, minuter och sekunder.


På vissa modeller går det att bifoga bilder tagna med kameran. De observationer som NFC har gjort tyder på att det går att vidarebefordra en bild som är mottagen från en annan användare. Det går därmed inte med säkerhet att säga vilken användare som tagit bilden. NFC har inte haft möjlighet att göra egna tester.

[9] Röstsamtal med internetteknik, samtal sker över internet och inte via det vanliga telenätet.

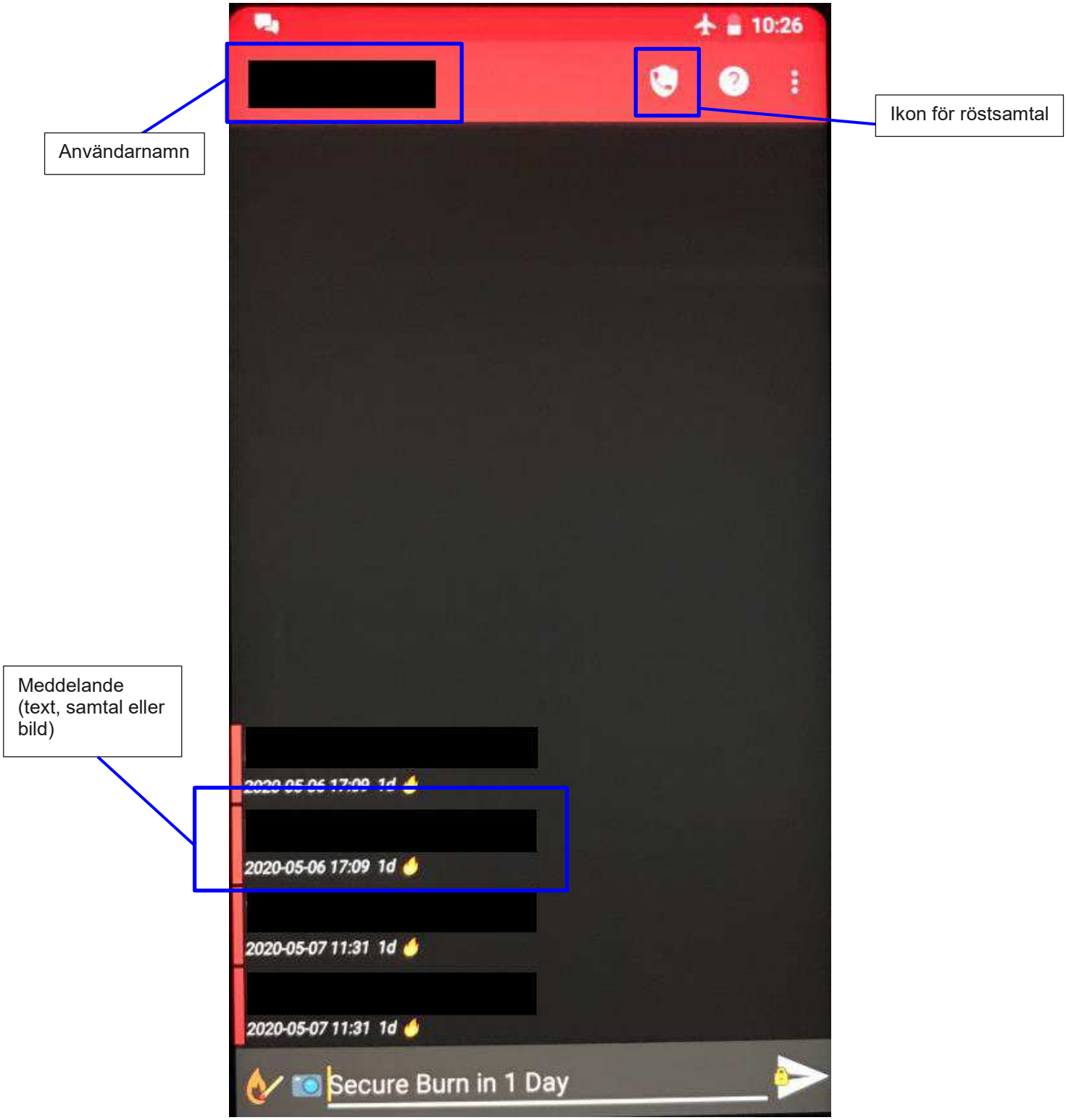


Bild 9 - Vy över en kontakt i applikationen Encrochat

3 Källor

[1] Paganini, P., Security Affairs (2017-03-10). The Dutch police decrypted a number of PGP messages sent by crooks through their BlackBerry mobile devices for the criminal investigation on Ennetcom. https://securityaffairs.co/wordpress/57036/cyber-crime/blackberry-pgp-messages [Hämtad 2020-09-08]. **Internetreferens**

[2] Cox. J., Vice (2017-03-09). Dutch Cops Say They've Decrypted PGP Messages On Seized Server. https://www.vice.com/en_us/article/3dyaqk/dutch-cops-say-theyve-decrypted-pgp-messages-on-seized-server [Hämtad 2020-09-08]. **Internetreferens**

[3] Federal Bureau of Investigation. International Criminal Communication Service Dismantled (2018-03-16). https://www.fbi.gov/news/stories/phantom-secure-takedown-031618. [Hämtad 2020-09-15]. **Internetreferens**

[4] Vaas. L., Naked Security. 258,000 encrypted IronChat phone messages cracked by police (2018-11-09). https://nakedsecurity.sophos.com/2018/11/09/258000-encrypted-ironchat-phone-messages-cracked-by-police. [Hämtad 2020-09-15]. **Internetreferens**

[5] Khandelwal. S., The Hacker News. Dutch Police Seize Another Company that Sells PGP-Encrypted Blackberry Phones (2017-05-11). https://thehackernews.com/2017/05/police-blackberry-pgp-phones.html. [Hämtad 2020-09-15]. **Internetreferens**

[6] Vin Group. Vinsmart purchases intellectual property rights from BQ to produce Vsmart smartphone (2018-07-06). https://vingroup.net/tin-tuc-su-kien/bai-viet/2015/vinsmart-mua-ban-quyen-so-huu-tri-tue-tu-bq-de-san-xuat-dien-thoai-thong-minh-vsmart. [Hämtad 2020-09-17]. **Internetreferens**

nfc.polisen.se

Nationellt forensiskt centrum – NFC
581 94 Linköping, Telefon 010-562 80 20
e-post registrator.nfc@polisen.se

Swedish National Forensic Centre – NFC
SE-581 94 Linköping, Tel +46 10 562 80 20
e-mail registrator.nfc@polisen.se

Polisen

Polisen

PM EncroChat NOA

Signerat av

Signerat datum

Enhet	Diarienr
Region Mitt, Aktionsgrupp 1 Rgn Mitt	5000-K355469-21

Orginalhandlingens förvaringsplats	Datum	Tid
	2021-04-15	08:36

Involverad personal	Funktion
Johan Ericson	Uppgiftslämnare

Polisen

PM

Datum
2021-01-12

Diarienr (åberopas)
A018.119/2021

Saknr
403

Polismyndigheten
Nationella operativa avdelningen

EncroChat

Inledning

Sedan april 2020 har svensk polis via Nationella operativa avdelningen (Noa) deltagit i en insats ledd av Europol i en gemensam operation med Frankrike och Nederländerna mot företaget EncroChat. Detta dokument syftar till att ge en bakgrund till den europeiska operationen samt att ge en översiktlig bild av den svenska insatsen.

Bakgrund

Operationen inkluderar ett antal länder, däribland Sverige. Samverkan inleddes efter att brottsbekämpande myndigheter medvetandegjordes om att modifierade telefonenheter hade försetts med dubbla operativsystem varvid det ena med krypterade applikationer för kommunikation. Enligt Europol har den krypterade lösning/tjänst som EncroChat erbjudit i hög utsträckning och nära nog uteslutande använts av kriminella i syfte att kunna begå brott. Franska myndigheter beslutade därför att inleda ett ärende vid Eurojust och vände sig i ett första skede till Nederländerna för en bilateral samverkan i operationen. Det blev genom denna samverkan till slut möjligt att genom en teknisk lösning ta sig förbi krypteringstekniken och få åtkomst till användarnas korrespondens och annan information. Uppgifterna har tagits fram med stöd av fransk lag.

Europol har i realtid bearbetat och analyserat mottagna meddelanden och uppgifter. Genom arbetet har de brottsbekämpande myndigheterna lyckats fånga upp information som sedan delats med ett antal länder bland annat Sverige. Det rör sig om miljontals meddelanden som utväxlats mellan användarna av enheterna där grova brott planerats. Encrochattarna har till stor del kunnat följas i realtid även av myndigheter i olika länder, för Sveriges del underrättelseenheten vid Noa.

Sverige

Det svenska deltagandet påbörjades i början av april 2020 under ledning av Noa:s underrättelseverksamhet. Initialt koncentrerades samtliga resurser till att förhindra mord, våld och annan grov kriminell verksamhet på olika platser i Sverige.

Den information som svensk underrättelseverksamhet har haft och fortfarande har tillgång till omfattar i huvudsak perioden 1 april till 13 juni 2020. Det finns dock i undantagsfall information som härstammar från tiden före och efter dessa datum.

Svenska myndigheter har inledningsvis enbart fått använda materialet för att inleda förundersökning och för att på andra sätt förhindra grova brott.

Att därefter använda materialet i en förundersökning/rättegång som bevisning förutsätter att en europeisk utredningsorder, EIO, utfärdats och skickats via Eurojust. Efter tillstånd av behörig fransk myndighet överlämnas materialet varvid all information delges svensk polis eller annan berörd brottsbekämpande myndighet. Materialet får delas som överskottsinformation till andra svenska förundersökningar.

Europa

Enligt Europols hemsida har informationen från telefoner och konton varit betydelsefull i och för ett stort antal pågående europeiska brottsutredningar vilket bland annat har lett till att brottslig verksamhet avbrutits genom att förhindra till exempel våldsanvändning, mordförsök och storskaliga narkotikatransporter. Ett stort antal misstänkta EncroChat-användare har gripits i ett flertal europeiska länder, bland annat Sverige.

I Sverige har arbetet initialt styrts av Noa:s Underrättelseenhet. När operationen övergick till primärt brottsutredande inleddes nära samverkan med Noa:s Utredningsenhet som ansvarar för att koordinera förundersökningsarbetet på nationell nivå. Bedömningen är att information från Encrochattarna kommer att användas inom ett större antal svenska förundersökningar under ledning av åklagare, polis och tull.

Nedstängning av EncroChat

Möjligheten att kunna följa EncroChat-meddelanden avstannade i princip helt den 13 juni 2020 i samband med att företaget insåg att myndighet/er tagit sig in på plattformen. EncroChat sände då ett varningsmeddelande till alla användare och rådde dessa att omedelbart göra sig av med sina telefoner.

Vad är EncroChat?

Till detta dokument biläggs ett dokument från Nationellt forensiskt centrum, NFC, Informationsteknikseksektionen, som i sitt sammanfattande dokument ger en teknisk beskrivning och analys av enheternas och EncroChats funktionaliteter.

Polisen

Encrochat-utredningen i Frankrike

Signerat av

Signerat datum

Enhet	Diarienr
Region Mitt, Aktionsgrupp 1 Rgn Mitt	5000-K355469-21

Orginalhandlingens förvaringsplats	Datum	Tid
	2021-05-17	08:20

Involverad personal	Funktion
Johan Ericson	Uppgiftslämnare

Berättelse

Dokumnet från www.eurojust.europa.eu/fr/encrochat-investigation-france översatt av Polismyndigheten, NOA.

EncroChat-utredningen i Frankrike

Ärendets uppkomst samt kronologisk redogörelse

Inom ramen för en förundersökning vid den interregionala specialdomstolen (JIRS) vid regiondomstolen i Lille och som numera bedrivs av undersökningsdomarna med anledning av att en rättslig förunderökning inletts den 28 maj 2020, vilken anförtrotts åt styrelsen för nationella gendarmeriet (Direction Générale de la Gendarmerie Nationale) samt av dess IT-brottscentrum C3N (Centre de lutte contre les criminalités numériques C3N), som har nationell behörighet, har förekomsten av en krypterad kommunikationslösning kunnat identifieras som saluförs under handelsbeteckningen **EncroChat** och används av kriminella organisationer.

2017, upptäckte avdelningen för elektronisk datateknik (Département Informatique Électronique (INL)) vid Institutet för brottsundersökningar vid Nationella gendarmeriet (Institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN)) telefoner som använder sig av den krypterade kommunikationstjänsten Encrochat. Fördjupad efterforskning inleddes i syfte att förstå hur den fungerade. Tack vare projekt CERBERUS, under gendarmeriets ledning och finansierad med EU-medel, snabbades i början av 2019 IRCGNs forskning på avseende dessa telefoner.

Nationella gendarmeriets kriminaltekniska dokumentation, liksom de undersökningar som gjorts vid rättsliga myndigheter, har parallellt påvisat återkommande fall av specifikt denna typ av krypterade telefoner inom ramen för ärenden rörande transport och olaglig narkotikahandel inom den organiserade brottsligheten.

Det framkommer dock av gendarmernas tekniska undersökningar att den krypterade kommunikationslösningen i fråga, ej redovisad i Frankrike, genomfördes via i Frankrike installerade servrar till förmån för kunder över hela världen. Genom utredningen har man lyckats sammanföra information om hur lösningen tekniskt fungerar, vilket lett till att en teknisk lösning kunnat upprättas. Tack vare denna har användarnas icke-krypterade kommunikationer kunnat inhämtas.

Att syftet med kommunikationslösningen EncroChat var att bistå kriminella organisationer stöddes av utredningen, bl.a. i och med återförsäljningsvillkoren avseende dessa telefoner, samt de tjänster som kunderna erbjöds för att garanteras anonymitet och straffrihet i händelse av identitetskontroll.

Det mycket stora antalet användare som ägnar sig åt brottslig verksamhet (över 90 procent i Frankrike, vilket motsvarar samtliga användare i egenskap av faktiska användare av terminalerna) gav i Frankrike upphov till att sidoutredningar inleddes vid de behöriga åklagarmyndigheterna.

Natten mellan den 12 och 13 juni 2020, skickade EncroChat ut en säkerhetsvarning till hela sin kundkrets i vilken de bl.a. informerade om att kommunikationslösningen utsatts för ”olagligt övertagande” av ”statliga organ”. Kunderna rekommenderades att bl.a. fysiskt göra sig av med sina terminaler (”*You are advised to power off and physically dispose your device immediatly”*).

Trots förekomsten av kriminell användning av Encrochatterminalerna, önskar de franska myndigheterna att de användare som säger sig handla i god tro och som skulle vilja få sina personuppgifter borttagna från det rättsliga förfarandet ska kunna inlämna en begäran om detta till utredningsavdelningen. Likaledes, i samband med att organisationen som ansvarar för driften av Encrochats tekniska lösning varnade sina användare för påstått ”olagligt” agerande mot deras servrar, är alla personer i egenskap av chef, företrädare eller förvaltare för företagen bakom den här tjänsten välkomna att ge sig till känna och lägga fram sina argument inför gendarmeriet på följande adress contact.encrochat@gendarmerie.interieur.gouv.fr

Rättslig ram

Tvärtemot vad Encrochat och vissa av deras hörda användare påstår och som spridits av internationella medier, har den franska utredningen bedrivits i enlighet med tillämpliga rättsregler.

- **Rättslig ram: upptagning av elektroniska uppgifter, en särskild utredningsmetod som föreskrivs i fransk lagstiftning**

Artikel 706-102-1 i den franska straffprocesslagen

”En teknisk lösning får inrättas i syfte att bereda åtkomst, överallt, utan de berörda personernas samtycke, till elektroniska uppgifter, och spela in, förvara och överföra dessa, så som de lagrats i ett datorsystem, visats på en skärm för användaren av ett system för automatiserad behandling av uppgifter, matats in genom inknappning av tecken eller emottagits och skickats av kringutrustning.

Allmänna åklagaren eller undersökningsdomaren kan utse alla personer som är bemyndigade och som finns med i förteckningen enligt artikel 157, att utföra de tekniska åtgärder som gör det möjligt att upprätta den tekniska lösning som anges i första stycket i denna artikel. Allmänna åklagaren eller undersökningsdomaren kan även föreskriva att statliga resurser som är föremål för nationell försvarssekretess används i enlighet med del 1, avdelning IV, kapitel 1”.

- **En strängt begränsad åtgärd**

→ har godkänts och kontrolleras av frihets- och häktningsdomaren (juge des Libertés et de la Détention) inom ramen för brottsutredningen och, sedan förundersökningen inleddes den 28 maj 2020, av de för ärendet gemensamt ansvariga undersökningsdomarna.

Artikel 706-95-12 i den franska straffprocesslagen

De särskilda utredningsmetoderna får användas:

1 Under utredningen: av frihets- och häktningsdomaren (juge des libertés et de la détention) på begäran av allmänna åklagaren;

2 Under förundersökningen: av undersökningsdomaren, efter yttrande från allmänna åklagaren.

Artikel 706-95-14 i den franska straffprocesslagen

”Dessa särskilda utredningsmetoder sker **under ledning och övervakning av den domare som har godkänt dem. Denna domare får när som helst beordra att dessa avbryts.**

Frihets- och häktningsdomaren (juge des libertés et de la détention) underrättas utan dröjsmål av allmänna åklagaren om de gärningar som begåtts. De protokoll som upprättats för att verkställa frihets- och häktningsdomarens beslut delges henne/honom.

Om frihets- och häktningsdomaren anser att åtgärderna inte genomförts i enlighet med hennes/hans godkännande eller om de bestämmelser som fastställts i denna lagsamling inte har iakttagits, beordrar hon/han att protokollen och de inspelningar som gjorts destrueras. Hon/han avgör målet genom motiverat beslut och delger allmänna åklagaren detta. Allmänna åklagaren kan inom tio dagar efter delgivningen överklaga domen till domstolschefen.

För att åtgärderna inte ska bli ogiltiga, får deras enda syfte vara att undersöka och fastställa de brott som avses i domarens beslut. Den omständigheten att dessa åtgärder visar på andra brott än de som avses i domarens godkännande innebär inte att de inte får användas i andra utredningar."

- Angående den tekniska lösningen:

→ allt utlämnande av uppgifter rörande den tekniska lösningen i fråga är straffbart enligt fransk lag (art. 413- 9 samt 413-10 i franska strafflagen), det kan dock preciseras att följande har genomförts:

- tack vare en teknisk lösning har åtkomst möjliggjorts, på ett icke-krypterat sätt, till kommunikationer tillhörande ett stort antal tekniker och användare, inblandade i brottslig verksamhet, av denna kommunikationslösning som avsiktligt ställts till kriminella organisationers förfogande;

- en teknisk lösning för vilken "statliga resurser som är föremål för nationell försvarssekretess" har föreskrivits med stöd av artikel 706-102-1 i straffprocesslagen;

- en lösning vars utformning och mekanism omfattas av den nationella försvarssekretessen, men som emottagits och använts av ett enligt lag bemyndigat organ att göra detta, dvs den Centrala kriminalunderrättelsetjänsten vid Nationella Gendarmeriet (Service Central de Renseignement Criminel de la Gendarmerie Nationale (SCRC)), Nationella Gendarmeriets kriminalavdelning (Pôle Judiciaire de la Gendarmerie Nationale (PJGN)), i enlighet med art. D15-1-6 i straffprocesslagen.

Krypterade uppgifter

Mobilisering av Nationella gendarmeriet:

Den 15 mars 2020, beslutade Kriminalpolisavdelningen (Sous-Direction de la Police Judiciaire (SDPJ)) om att en nationell utredningsgrupp skulle bildas. Den var placerad i Pontoise, vid IT-brottscentret C3N (Centre de lutte Contre les Criminalités Numériques C3N) och består av en kommandocentral (KC) samt olika utredningsgrupper.
Gruppen har fått förstärkning av erfarna utredare från sektionen Sections de Recherches från hela Frankrike samt från de 4 centralbyråerna (OCLTI, OCLAESP, OCLDI, OCLCH), och består idag av 60 gendarmer som anlitats på heltid i uppdrag att analysera data samt tekniska undersökningar och rättsliga utredningar. De avsevärda materiella och mänskliga resurser som tagits i anspråk visar hur viktiga utredningarna är och hur viktigt det är för Nationella gendarmeriet att nå framgång i detta.

> + 2000 handlingar i målet;
> 360 handlingar kriminalteknisk bevisning från kriminaltekniker och forensiker.

Kronologisk redogörelse för ärendet

15 november 2018: C3N inleder en brottsutredning - de första tekniska undersökningarna;

7 december 2018: C3N åläggs av den interregionala specialdomstolen vid regiondomstolen i Lille (JIRS) att ta sig an ärendet under brottsrubriceringarna nedan:

- kriminell sammanslutning i syfte att begå brott som bestraffas med fängelse i 10 år;
- tillhandahållande av en kryptologisk lösning som inte enbart säkerställer funktioner för autentisering och integritetskontroll utan föregående tillkännagivande;
- överföring av en kryptologisk lösning som inte enbart säkerställer funktioner för autentisering och integritetskontroll från en av medlemsstaterna i Europeiska unionen utan föregående tillkännagivande;
- införsel av en kryptologisk lösning som inte enbart säkerställer funktioner för autentisering och integritetskontroll från en av medlemsstaterna i Europeiska unionen utan föregående tillkännagivande.

10 april 2020: undertecknande om Gemensam utredningsgrupp (JIT) mellan de berörda franska och nederländska rättsliga myndigheterna under Eurojusts ledning samt med stöd från Europol;

28 maj 2020: förundersökning vid JIRS i Lille inleds avseende följande punkter:

- kriminell sammanslutning i syfte att begå brott som bestraffas med fängelse i tio år, i förevarande fall och närmare bestämt de narkotikabrott avseende olaglig narkotikahandel som avses i artikel 222-37 i strafflagen, de grova penningtvättsbrotten, brotten avseende innehav, förvärv och överlåtelse av vapen i kategorierna A eller B;
- förvärv, transport, innehav och utbjudande eller överlåtelse av narkotiska preparat,
- organiserad införsel av narkotiska preparat;
- förvärv och innehav av krigsmateriel, vapen, ammunition, väsentliga delar i kategorierna A eller B;
- penningtvätt genom investeringstransaktioner, döljande eller omvandling av vinning som härrör från olaglig narkotikahandel;
- grov penningtvätt i organiserad form genom investeringstransaktioner, döljande eller omvandling av vinning som härrör från brott;
- tillhandahållande av en kryptologisk lösning som inte enbart säkerställer funktioner för autentisering och integritetskontroll utan föregående tillkännagivande;
- överföring av en kryptologisk lösning som inte enbart säkerställer funktioner för autentisering och integritetskontroll från en av medlemsstaterna i Europeiska unionen utan föregående tillkännagivande;
- införsel av en kryptologisk lösning som inte enbart säkerställer funktioner för autentisering och integritetskontroll från en av medlemsstaterna i Europeiska unionen utan föregående tillkännagivande.

BILAGOR

- **Interregionala specialdomstolen vid regiondomstolen i Lille**

Interregionala specialdomstolen vid regiondomstolen i Lille, en av de 8 JIRS-domstolarna som täcker hela Frankrike, är behörig i kampen mot brott som härrör från den organiserade brottsligheten och den grova ekonomiska brottsligheten. Dess verksamhetsområde täcker appellationsdomstolarna i Douai, Rouen, Amiens och Reims.

Dess materiella kompetensområde är i egenskap av detta samverkande med dess verksamhetsområden och kan således behandla mycket komplexa ärenden.

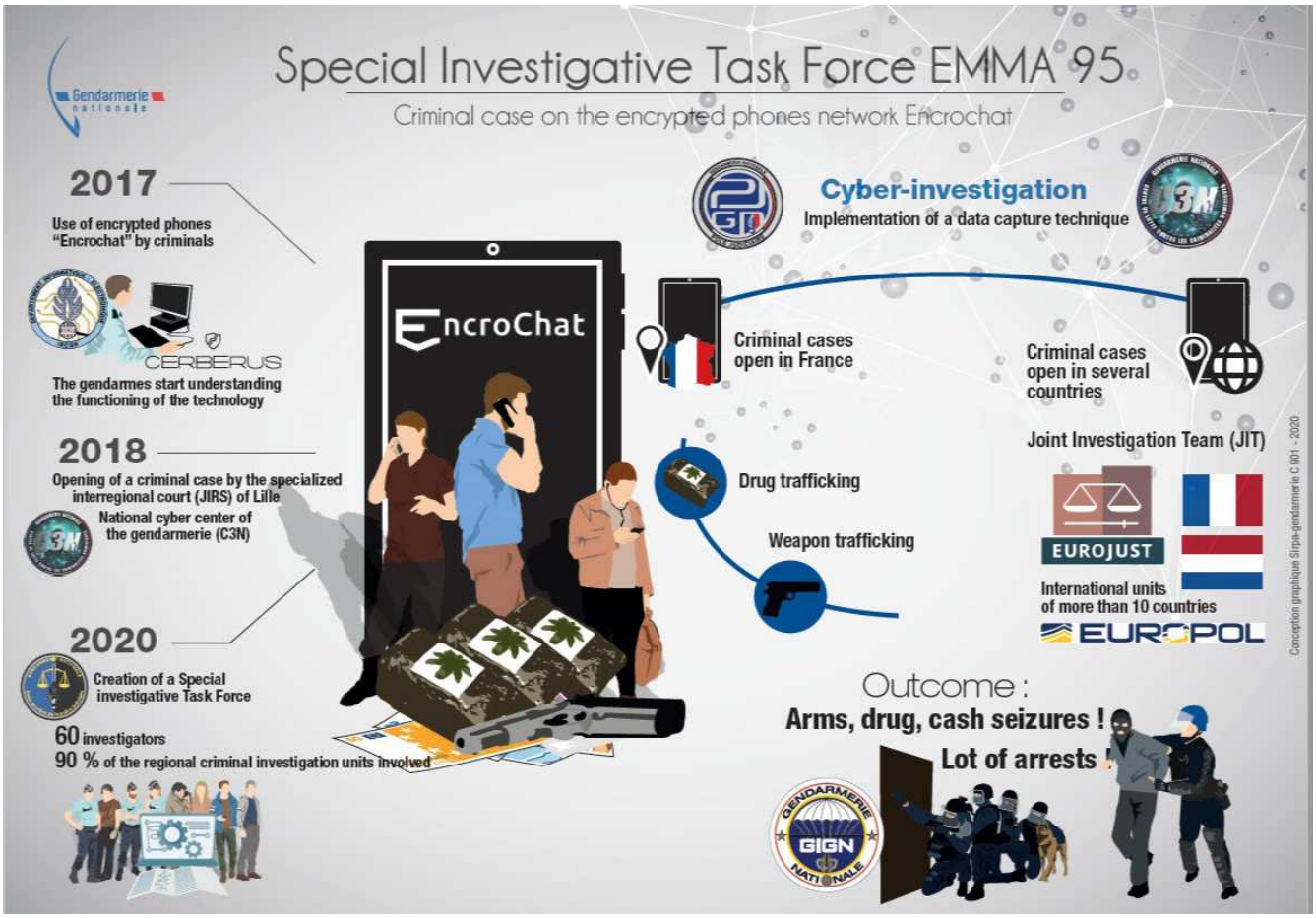
Interregionala specialdomstolen vid regiondomstolen i Lille har inlett en förundersökning gällande den krypterade kommunikationslösningen EncroChat med anledning av lokalisering av de servrar som säkrar processen.

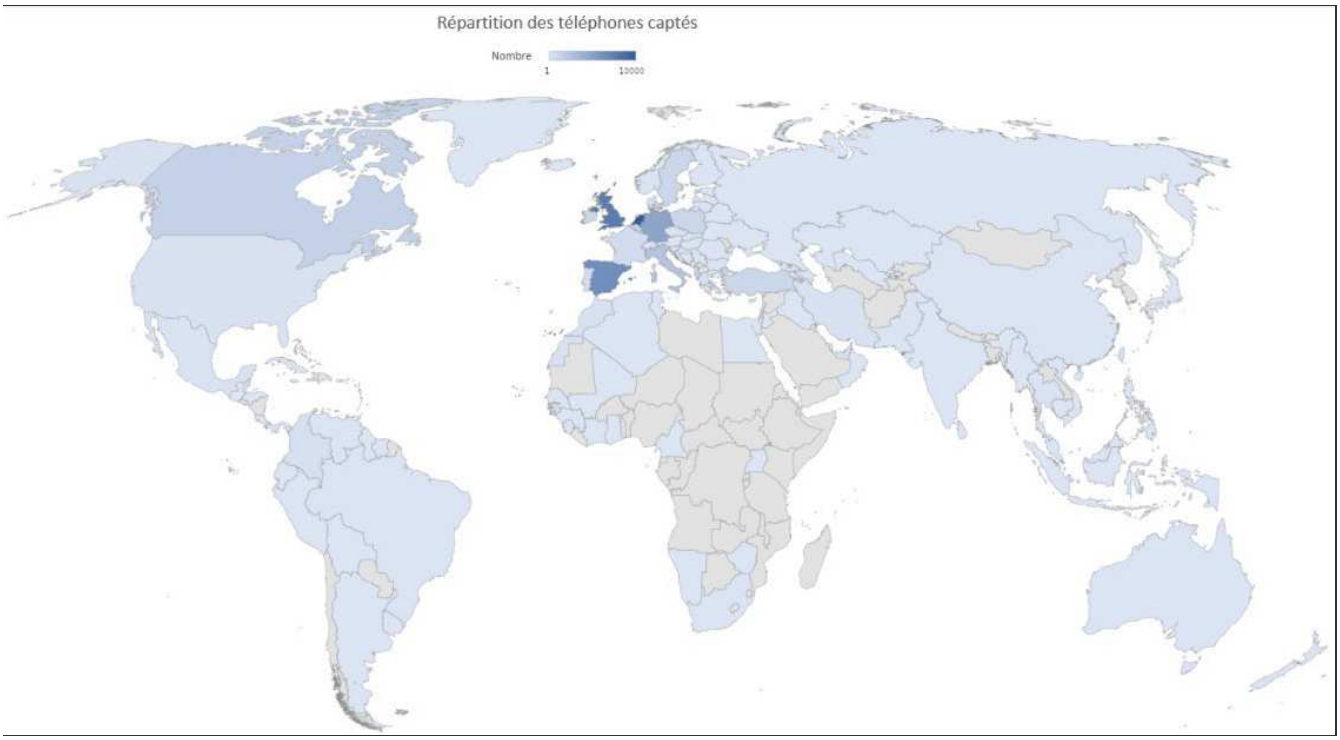
- **<u>Den gemensamma utredningsgruppen</u>**

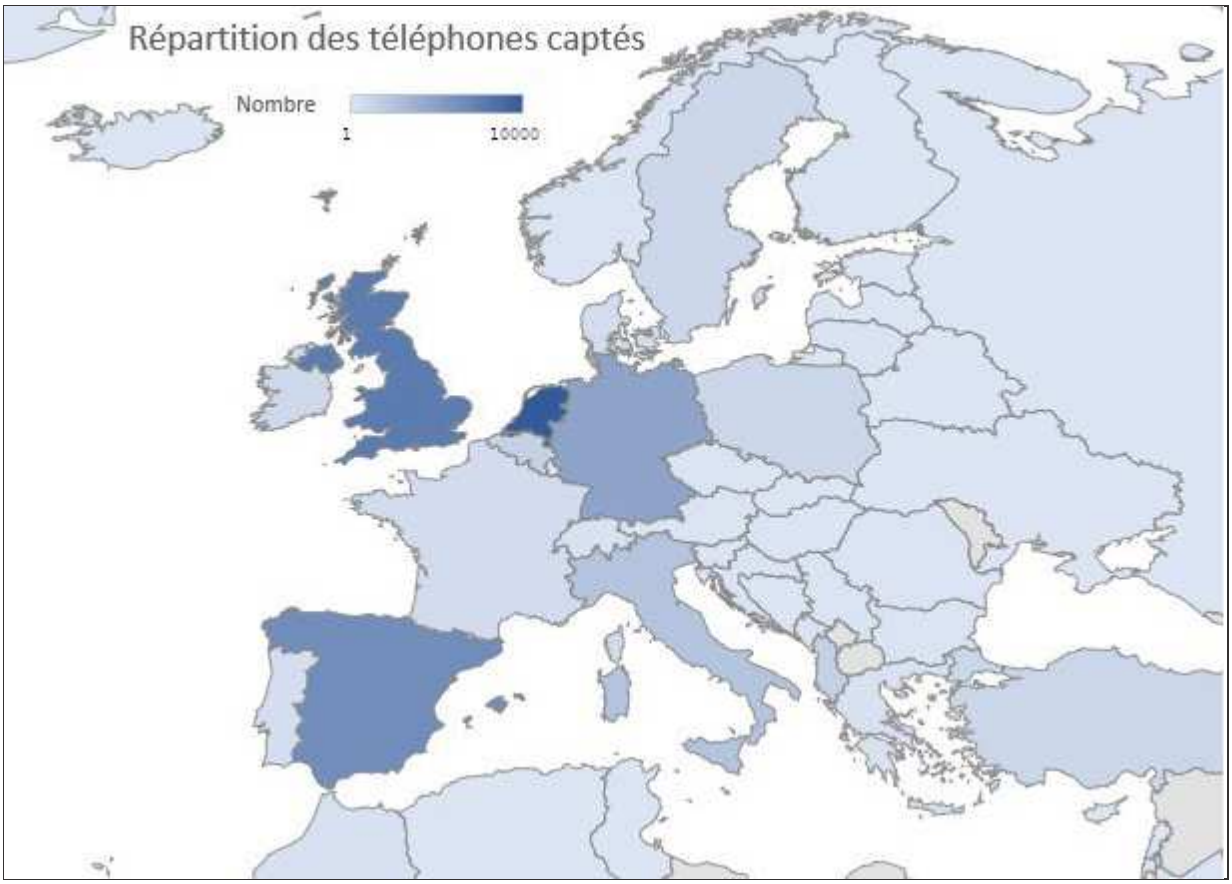
De gemensamma utredningsgrupperna har sitt ursprung i art. 13 i Konventionen om ömsesidig rättslig hjälp i brottmål som undertecknades i Bryssel, den 29 maj 2000, mellan de europeiska medlemsstaterna, samt i rambeslutet av den 13 juni 2002.

I enlighet med artiklarna 695-2 till 695-3 i strafflagen, gör de gemensamma utredningsgrupperna det möjligt att utveckla gemensamma utredningsstrategier, samt att ha gemensamma mål i kampen mot den gränsöverskridande organiserade brottsligheten. Grupperna för samman domare och utredare från två länder i en och samma enhet i ett ärende av gemensamt straffrättsligt intresse för de båda länderna. Denna mekanisms stora flexibilitet gör det möjligt för de rättsliga myndigheterna och för de berörda organen att utbyta underrättelser, bedriva gemensamma utredningsinsatser samt samordna lagföring i de båda länderna.

Den gemensamma utredningsgruppen kan endast upprättas inom ramen för redan existerande rättsliga förfaranden, brottsutredningar, polisutredningar eller förundersökningar. Initiativ till att bilda en utredningsgrupp kan tas av allmänna åklagaren, förundersökningsdomaren eller på begäran av rättsliga myndigheter i en eller flera medlemsstater.


Special Investigative Task Force EMMA 95
Criminal case on the encrypted phones network Encrochat
Gendarmerie nationale
2017
Use of encrypted phones "Encrochat" by criminals
CERBERUS
The gendarmes start understanding the functioning of the technology
2018
Opening of a criminal case by the specialized interregional court (JIRS) of Lille
National cyber center of the gendarmerie (C3N)
2020
Creation of a Special investigative Task Force
60 investigators
90 % of the regional criminal investigation units involved
EncroChat
Cyber-investigation
Implementation of a data capture technique
Criminal cases open in France
Criminal cases open in several countries
Drug trafficking
Weapon trafficking
Joint Investigation Team (JIT)
EUROJUST
International units of more than 10 countries
EUROPOL
Outcome :
Arms, drug, cash seizures !
Lot of arrests !
GENDARMERIE GIGN NATIONALE
Conception graphique Sirpa-gendarmerie © 001 - 2020


Répartition des téléphones captés
Nombre
1
10000


Répartition des téléphones captés
Nombre
1
10000

Polisen

Polismyndigheten

PM

Datum
2021-05-30

Diarienr (åberopas)
A352.681/2021

Positioneringar i Encrochatmaterial

Detta dokument beskriver kort vad det generellt innebär att en mobiltelefon är positionerad utifrån dess kontakt med telenätet. Dessutom förklaras även denna innebörd utifrån det material om Encrochat-telefoner som svensk polis fått tillgång till inom ramen för Op. Robinson.

Telefonterminologi

IMEI-nummer

Ett *IMEI-nummer* är en unik 15-siffrig kod som identifierar en mobiltelefon. IMEI-numret är knutet till själva hårdvaran, det vill säga mobiltelefonen, och är uppbyggt så att telefonmodell och telefontillverkare kan tas fram baserat på information som finns i IMEI-numret.

IMSI-nummer

Ett *IMSI-nummer* är ett unikt nummer som identifierar ett mobilabonnemang. Numret finns lagrat på SIM-kortet och är inte knutet till mobiltelefonen den sitter i. Från IMSI-numret kan information om vilket land och operatör ett visst IMSI-nummer tillhör tas fram.

Basstation

En *basstation* har *antenner* som förmedlar radiovågor till och från mobiltelefoner för att de ska kunna ringa och ta emot samtal, skicka och ta emot sms eller surfa på internet. Basstationer kan se ut på olika sätt men är ofta placerade högt upp, på ett hustak eller en höjd, och ofta på en ställning. Detta för att signalerna ska få så god räckvidd som möjligt.

Basstationens täckningsområde, det vill säga det geografiska området i vilken en mobiltelefon som kopplar upp mot den specifika basstationen teoretiskt kan befinna sig, delas oftast upp i *celler*. Varje cell har ett unikt id. Beroende på nätverk, exempelvis 4G eller 3G, kallas detta id för olika saker. I detta PM benämns detta unika ID-nummer för *Cell ID*.

Cell ID

Varje cell i det globala mobiltelenätet identifieras av ett ID-nummer (Cell ID). Ur Cell ID kan land, operatör, basstation och Cell ID utläsas. Genom att slå upp ett Cell ID i en databas går det att få fram geografisk koordinat för var basstationen är placerad samt riktning den aktuella antennen pekar ut från basstationen med.

Noa 2021-05-30

Generellt om positioner utifrån en mobiltelefons kontakt med telenätet

En uppgift om att en viss mobiltelefon har kopplat upp mot en viss basstation är ofta uttryckt genom att ett unikt id av den specifika telefonen ifråga, exempelvis IMEI-nummer eller IMSI-nummer, vid en viss tidpunkt eller under ett visst tidspann har kopplat upp mot en specifik cell i ett telefonnätverk, identifierbar genom ett unikt Cell ID.

Källan till en positionsuppgift som länkar samman en telefon med ett Cell ID kan variera. Det kan röra sig om uppgifter från en applikation nedladdad på telefonen i fråga, systemuppgifter från telefonen eller från telefonoperatören, för att nämna några exempel på källor.

Positioneringsuppgifter utifrån en mobiltelefons kontakt med telenätet lämnade från svenska teleoperatörer kommer från de loggar dessa operatörer har för att registrera den teletrafik som sker. Teletrafik i form av samtal och sms loggas på ett sätt som gör att det framgår tydligt att exakt vid en specifik tidpunkt kopplar telefonen upp mot en antenn som pekar ut i den här specifika cellen.

Svenska teleoperatörer har däremot signalerat att positioneringsuppgifterna de lämnar ut kopplade till datatrafik bygger på systemloggar som inte alltid möjliggör samma tydliga tolkning att varje registrering ger en exakt tid för när telefonen kopplade upp mot en antenn som pekar ut i en specifik cell. För att korrekt tolka dessa positioneringsuppgifter behöver därför ytterligare analys genomföras för att säkerställa vilka uppgifter om positioneringen som är tillförlitliga.

Positioner i Encrochat-materialet

Positionsuppgifterna som finnas att tillgå i materialet om Encrochat-telefoner kopplar samman en viss telefon, identifierad genom det unika Encrochat-användarnamnet, IMEI-numret och IMSI-numret, vid en viss tidpunkt och mot ett visst så kallat Antenna ID, eller som benämningen i detta PM, Cell ID. Källa till dessa positionsuppgifter är en polismyndighet i ett annat land.

När den specifika cellen som ett Cell ID refererar till är identifierat kan cellen representeras visuellt på en karta på olika sätt. Vanligt på polismyndigheten är att markera ut positionen för basstationen som cellen tillhör och markera från basstationen i vilken riktning antennen pekar ut i cellen. På så sätt kan en god uppskattning göras inom vilket geografiskt område telefonen vid tillfället har befunnit sig.

Fransk polis har överlämnat Encrochat-materialet med avsikten att det ska kunna användas i förundersökning. Överlämnande har gjorts utan något medskick att uppgifterna inte är tillförlitliga.

Nationellt forensiskt centrum – NFC

Polisen

Förkonfigurerade enheter

Sammanfattad information om enheter med applikationen GhostECC konfigurerade med BlackBerry UEM

NFC Notat 2022:3

Informationstekniksektionen

Utgivare
Nationellt forensiskt centrum – NFC
581 94 Linköping
Tfn 010-562 80 20
E-post registrator.nfc@polisen.se
www.nfc.polisen.se

Produktion Informationstekniksektionen, Polismyndigheten, 2022-02-01
Upplaga Digital version

Sammanfattning

Behovet av att i kriminella kretsar kommunicera digitalt har ökat i takt med teknikutvecklingen. Sedan introduktionen av Encrochat i slutet av 2010-talet har kommunikation via krypterade chatt-applikationer varit en vanlig förekommande kommunikationsform. Encrochat var inte bara en chatt utan även en enhetshanteringstjänst där konton och abonnemang kontrollerades centralt.

Liknande enhetshanteringstjänster används av legitima företag för att trygga säkerheten företagets mobila enheter som används av de anställda. En sådan enhetshanteringstjänst erbjuds av det kanadensiska tjänsteföretaget Blackberry. I denna rapport redovisas sammanfattad information om telefoner med chatt-applikationen GhostECC som använder Blackberrys enhetshanteringstjänst.

Innehållsförteckning

1 Inledning

1.1 Bakgrund

Smarttelefoner förkonfigurerade för säker kommunikation har varit vanligt förekommande i brottsutredningar som är kopplade till någon form av organiserad brottslighet under lång tid. Sedan tidigt 2010-tal har olika telefonmodeller och kommunikationstjänster med varierande bakomliggande teknisk lösning påträffats i samband med beslag. Det som förenar dessa kommunikationstjänster är att telefonerna är konfigurerade på ett sådant sätt att de företrädesvis används för krypterad kommunikation.

Fram till 2017 var det främst telefoner av märket BlackBerry som togs i beslag i Sverige och många av telefonerna hade sitt ursprung från det nederländska företaget Ennetcom. Som kommunikationsform användes krypterad e-post där meddelandet raderades efter en förutbestämd tid. Ennetcoms servrar togs i beslag i april 2016 och senare kunde ett antal miljoner meddelanden dekrypteras [1] [2]. Liknande beslag av servrar har gjorts på tjänster som Phantom Secure [3], IronChat [4] och PGP Safe [5].

Under perioden 2017 till 2020 var det främst enheter med en variant av operativsystemet Android, vid namn Encrochat OS, som påträffades i brottsutredningar [6]. I juli 2020 gick Europol ut med en pressrelease där man informerade att man tillsammans med ett antal medlemsländer lyckats läsa av och analysera kommunikationen i Encrochat under ett antal månader [7]. I mars 2021 meddelade Europol att man lyckats övervaka tjänsten SkyECC och dess cirka 70 000 användare [8]. Cirka tre månader senare blev det känt att kommunikationstjänsten ANØM utvecklats och i hemlighet drivits av federal polis i USA och Australien[1]. Vid avslöjandet i juni 2021 hade uppemot 12 000 enheter använt tjänsten världen över [9].

Ett incitament för att sälja dessa typer av enheter är att enheterna och dess abonnemang har en hög kostnad och den potentiella vinstmarginalen är stor. För att hantera och skapa en vinstdrivande verksamhet kring försäljning och förvaltning används oftast en central enhetshanteringstjänst som exempelvis Blackberry UEM.

1.2 Syfte

Att förse Nationellt Forensiskt Centrums uppdragsgivare med en övergripande bild över hur enheter styrda med enhetshantering använts, konfigurerats och distribuerats. Viss informationen från NFC IT-notat 2021-1 [10] har överförts till detta dokument då både SkyECC och GhostECC nyttjat Blackberry UEM som enhetshanteringstjänst.

1.3 Avgränsning

I denna rapport beskrivs enhetshantering i allmänhet och enheter som säljs som GhostECC i synnerhet. Då ett flertal applikationer kan användas på dessa enheter beskrivs applikationen Ghost endast i korthet.

Hur enheterna specifikt kan användas är strikt kopplad till vilken form av tjänst som används och hur säkerhetspolicyn är konfigurerad. NFC uttalar sig om det som är observerat vilket inte utesluter annan funktionalitet.

[1] Operationen var ett samarbete mellan FBI (Federal Bureau of Investigation) och AFP (Australian Federal Police).

2 Analys

Mobilenheter som är konfigurerade med en mobil enhetshanteringstjänst är styrda med hjälp av särskild programvara samt regler som implementerar en säkerhetspolicy. Mobil enhetshantering är ett vanligt verktyg för IT-avdelningar inom företag och den offentliga sektorn och gör det möjligt att övervaka, hantera och säkra företagets mobila enheter.

Förkonfigurerade enheter som marknadsförs som GhostECC använder Blackberrys enhetshantering för att styra och kontrollera hur enheterna används. Uppsatta regler i enhetshanteringen styr bland annat vilka applikationer som ska finnas tillgängliga på enheten samt användarens möjlighet att installera nya applikationer.

2.1 Begrepp

Nedan redogörs närmre för ett antal begrepp som används i detta dokument.

- **Android**
  Ett operativsystem med öppen källkod för bland annat smarttelefoner och surfplattor. Operativsystemet används av flera tillverkare som till exempel Google och Samsung.

- **Elliptic-curve cryptography (ECC)**
  Ett antal kommunikationsapplikationer använder begreppet ECC i sitt applikationsnamn, exempelvis GhostECC. Detta är ett sätt att tala om att applikationen använder en säker kryptering. ECC är ett sätt att implementera asymmetrisk kryptering och kan som sådan användas för bland annat krypterad kommunikation. I dag använder de mest kända chatt-applikationerna någon form av ECC i sin konfiguration [9].

- **Förkonfigurerade enheter**
  Ett samlingsnamn som används av Nationellt Forensiskt Centrum. Definition: ”Förkonfigurerade enheter är enheter som används av kriminella nätverk med syfte att dölja kommunikation. Enheterna har olika fabrikat och teknisk lösning.”

- **Google Play Store**
  En digital distributionstjänst som drivs och utvecklas av Google. Det är Androids officiella butik för att ladda ned och uppdatera applikationer.

- **Mobile Device Management (MDM)**
  Förenklat och något kortfattat kan Mobile Device Management beskrivas som de tjänster som gör det möjligt för ett företag att kontrollera hur organisationens mobila enheter får användas. Inom MDM kan enheter lokaliseras, låsas och raderas [8].

- **Unified Endpoint Management (UEM)**
  UEM är en vidareutveckling av MDM som tillåter kontroll och styrning för ökad säkerhet hos en större flora av klienter som mobilenheter, surfplattor, bärbara och stationära datorer och på senare tid även IoT-enheter (Internet of Things).

2.2 Blackberry

Blackberry är ett kanadensiskt företag känt för sitt fokus på säkra produkter. De tjänster som Blackberry erbjuder används företrädesvis av organisationer i Nordamerika. En av de tjänster som Blackberry erbjuder är Blackberry UEM som på sin hemsida beskrivs:

> ”…[tjänsten] ger en omfattande enhets-, applikation- och innehållshantering med integrerade säkerhets och anslutningsmöjligheter och hjälper dig hantera iOS-, macOS-, Android-, Windows 10- och Blackberry 10-enheter för din organisation.”[2]

Organisationer som är i behov att administrera mobila enheter kan ansluta sig till Blackberry UEM och få tillgång till en helhetslösning. För att kunna koppla mobila enheter till enhetshanteringen behöver organisationen både följa Blackberrys krav och riktlinjer och därtill den specifika enhetsfabrikörens krav. För till exempel Apple-enheter behöver organisationen även vara ansluten till Apples företagslösning för tillgång till Blackberrys tjänst.

I korthet så registreras enheten i Blackberrys system och en klient installeras på enheten. Vilka applikationer som tillåts på enheten styrs via administrationsgränssnittet i Blackberry UEM (se Bild 1).

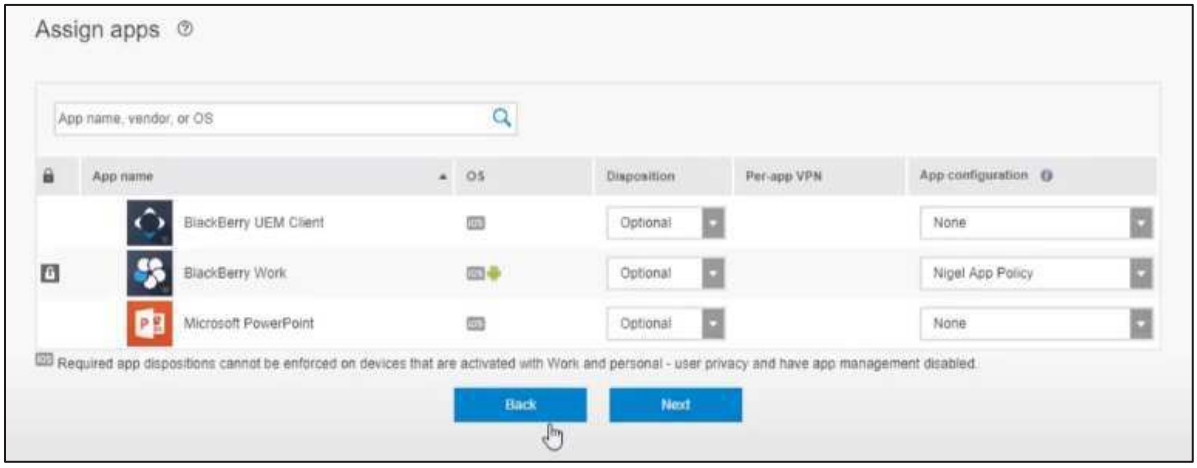


Bild 1 - Vy för att tilldela applikationer (Källa: Blackberrys användarmanual).

2.2.1 Blackberry-applikationer

Blackberry-applikationen UEM Client har påträffats på enheter med GhostECC (Bild 2). Denna applikation ser till att reglerna i den uppsatta säkerhetspolicyn följs.

Bild 2 - Ikon för Blackberrys applikation UEM Client (GhostECC).

[2] https://docs.blackberry.com/en/endpoint-management/blackberry-uem/12_13 (hämtad 2021-01-22)

2.3 Karaktär hos ärenden

Antalet beslagtagna telefoner konfigurerade med Encrochat minskade i antal under 2020 samtidigt som antalet förkonfigurerade telefoner med andra liknande tjänster ökade i brottsutredningar av samma karaktär.

I Sverige har majoriteten av påträffade enheter med GhostECC varit Android-enheter av tillverkarna Samsung eller Google. De ärenden där dessa telefoner påträffats har oftast varit knutna till någon form av organiserad brottslighet med brottsrubriceringar som bland annat:

- Mord eller dråp, misshandel med dödlig utgång
- Försök till mord eller dråp
- Försök, förberedelse och stämpling till mord eller dråp
- Brott mot narkotikastrafflagen
- Grovt vapenbrott

2.4 Operatör

Förkonfigurerade enheter använder vanligen endast datatrafik. Säkerhetspolicyn och det abonnemang som används hindrar användaren att ringa vanliga telefonsamtal. Funktionaliteten i dessa enheter är konfigurerad att endast använda datatrafik[3]. De SIM-kort som påträffats har obegränsad datamängd under den förbetalda abonnemangstiden. Majoriteten av de SIM-kort som påträffats har kommit från den spanska telekomföretaget Telefónica som marknadsförs via de egenägda operatörerna Movistar, O_2 och Vivo (Bild 3). SIM-kort med andra operatörer har påträffats till exempel KPN, Comviq eller Tre.

Bild 3 - Telefónica Global SIM

2.5 Pris

Priset för förkonfigurerade enheter varierar beroende på modell, antal och tidigare kontakt med distributören. Det kan dock konstateras att priset är markant högre än att köpa en liknande telefonmodell via vanliga inköpskanaler. Normalt brukar en förkonfigurerad telefon kosta mellan 10 000 och 20 000 SEK där abonnemangslängden vanligen är tre till sex månader.

[3] Vanligt förekommande begrepp är data-SIM, M2M-kort (Machine to machine) och telematikkort.

2.6 Applikationer

Säkerhetspolicyn i BlackBerry UEM styr bland annat vilka applikationer som finns förinstallerade, om användaren kan installera egna applikationer och vilka behörigheter applikationerna tillåts att ha. Enheter konfigurerade med GhostECC skiljer sig från tjänster som Encrochat, SkyECC och ANØM då användaren tillåts använda applikationer som finns i det officiella applikationsbiblioteket Google Play Store.

Bild 4 och Bild 5 visar exempel på applikationer som kan finnas förinstallerade på en GhostECC-telefon när användaren får tillgång till den. Observera att denna visualisering inte på något sätt är uttömmande så andra applikationer kan finnas installerade på andra GhostECC-enheter. Vissa applikationer kan finnas installerade för syns skull och stoppas av säkerhetspolicyn vid användande. Vanligen använda typer av applikationer är de för kommunikation samt applikationer för hantering av kryptovalutor.

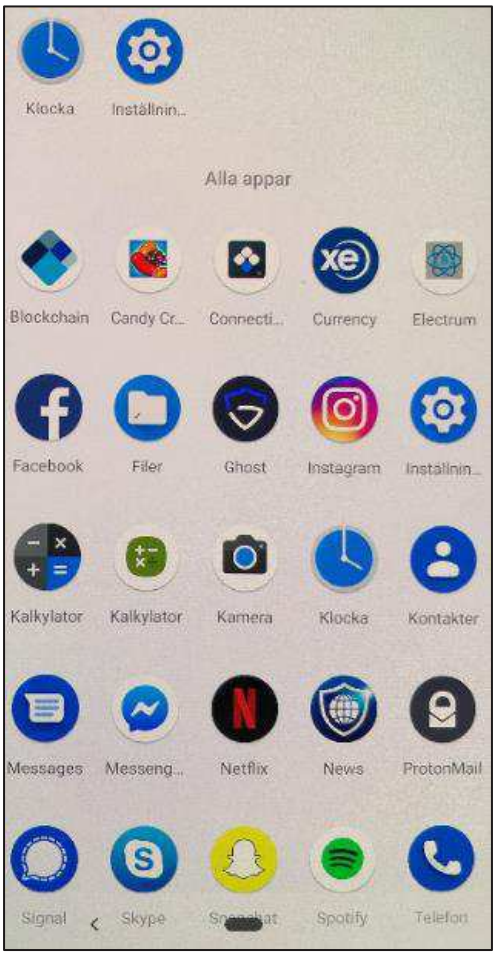


Bild 4 - Förinstallerade applikationer på GhostECC

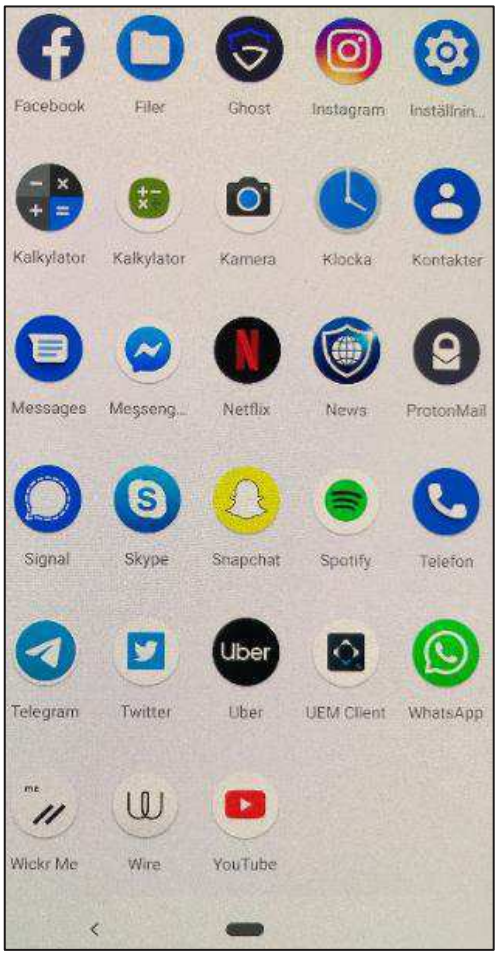


Bild 5 - Förinstallerade applikationer på GhostECC

2.6.1 Applikationen Ghost

På de flesta enheter med GhostECC konfigurerat finns även applikationen Ghost som är en chatt-applikation som endast finns på dessa typer av enheter. Användaren är inte bunden till att använda Ghost utan kan välja att använda någon annan chatt-applikation.

Applikationen Ghost har en chatt-funktion med möjlighet att ringa röstsamtal via enhetens dataanslutning. Likt många liknande applikationer finns även ett valv för lagring av anteckningar, chatt-meddelanden, bilder, filmer och röst-meddelanden.

3 Källor

[1] Paganini, P., Security Affairs (2017-03-10). The Dutch police decrypted a number of PGP messages sent by crooks through their BlackBerry mobile devices for the criminal investigation on Ennetcom. https://securityaffairs.co/wordpress/57036/cyber-crime/blackberry-pgp-messages [Hämtad 2020-09-08]. **Internetreferens**

[2] Cox. J., Vice (2017-03-09). Dutch Cops Say They've Decrypted PGP Messages On Seized Server. https://www.vice.com/en_us/article/3dyaqk/dutch-cops-say-theyve-decrypted-pgp-messages-on-seized-server [Hämtad 2020-09-08]. **Internetreferens**

[3] Federal Bureau of Investigation. International Criminal Communication Service Dismantled (2018-03-16). https://www.fbi.gov/news/stories/phantom-secure-takedown-031618. [Hämtad 2020-09-15]. **Internetreferens**

[4] Vaas. L., Naked Security. 258,000 encrypted IronChat phone messages cracked by police (2018-11-09). https://nakedsecurity.sophos.com/2018/11/09/258000-encrypted-ironchat-phone-messages-cracked-by-police. [Hämtad 2020-09-15]. **Internetreferens**

[5] Khandelwal. S., The Hacker News. Dutch Police Seize Another Company that Sells PGP-Encrypted Blackberry Phones (2017-05-11). https://thehackernews.com/2017/05/police-blackberry-pgp-phones.html. [Hämtad 2020-09-15]. **Internetreferens**

[6] Nationellt Forensiskt Centrum. Förkonfigurerade enheter – Sammanfattad information om Encrochat OS. NFC Notat, Informationstekniksektionen 2020:09. **Interna rapporter & Notat**

[7] Europol. Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe (2020-07-02). https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe. [Hämtad 2020-12-23]. **Internetreferens**

[8] Europol. New major interventions to block encrypted communications of criminal networks (2021-03-10). https://www.europol.europa.eu/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks [Hämtad 201-11-22]. **Internetreferens**

[9] Europol. 800 criminals arrested in biggest ever law enforcement operation against encrypted communication (2021-06-08). https://www.europol.europa.eu/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication [Hämtad 2021-11-22]. **Internetreferens**

[8] Cheuvront, D., Security Intelligence. Why UEM Is the New MDM: The Latest Stage in Enterprise Evolution (2018-07-03). https://securityintelligence.com/why-uem-is-the-new-mdm-the-latest-stage-in-enterprise-evolution. [Hämtad 2020-12-23]. **Internetreferens**

[9] Secure Messaging Apps Comparison (2021-01-19). https://www.securemessagingapps.com/ [Hämtad 2021-01-22]. **Internetreferens**

[10] Nationellt Forensiskt Centrum. Förkonfigurerade enheter – Sammanfattad information om enheter med applikationen SkyECC konfigurerade med Blackberry UEM. NFC Notat, Informationstekniksektionen 2021:01. **Interna rapporter & Notat**

nfc.polisen.se

Nationellt forensiskt centrum – NFC
581 94 Linköping, Telefon 010-562 80 20
e-post registrator.nfc@polisen.se

Swedish National Forensic Centre – NFC
SE-581 94 Linköping, Tel +46 10 562 80 20
e-mail registrator.nfc@polisen.se

Polisen

Polisen

PM

Datum
2021-03-03

Nationella operativa avdelningen, Noa
Utredningsenheten
Nationellt it-brottscentrum, SC3

Angående mobiltelefoner med GhostECC

Under 2020 har SC3 hanterat ett ökande antal beslag i brottsutredningar där enheten är av typen GhostECC.

Enligt hemsidan (http://ghostecc.com) erbjuder GhostEcc användaren att köpa en enhet som har:

- Oknäckbar kryptering av information.
- 100% Anonymitet.
- Secure Shredding, samtliga meddelanden som skickas eller tas emot raderas på ett sätt som ska göra det omöjligt att återskapa meddelanden.

Priserna för en enhet av typen GhostEcc ligger på mellan 12.000 – 15.000 SEK (2021-02-01).

Under sommaren 2020 kom fransk polis över information från tjänsten EncroChat, kort därefter stängdes tjänsten ned. EncroChat erbjöd en liknande lösning för kommunikation som GhostEcc.

Information från EncroChat har använts och används fortfarande i en stor mängd utredningar som drivs av svensk polis:

”*Hittills har totalt 125 fängelseår utdömts i Stockholmspolisens utredningar med bevisning från det krypterade verktyget Encrochat. Flera åtal och rättegångar om allvarlig brottslighet som mord, mordförsök, förberedelse till mord, allmänfarlig ödeläggelse, synnerligen grova narkotikabrott och människorov är att vänta framöver*” (citat från polisen.se)

Min uppfattning är att beslagen av telefoner med GhostECC ökat efter nedstängningen av EncroChat.

Med anledning av det höga priset, enhetens funktion och den miljö enheterna har beslagtagits i är min uppfattning att enheter av typen GhostECC i stor utsträckning används i syfte att underlätta och bedriva brottslig verksamhet.

Magnus Sandberg
Nationellt it-brottscentrum, SC3

Polisen

Bilaga - Skäligen misstänkt

Enhet
Region Mitt, Grova brott 1 PO Gävleborg

Diarienr
5000-K355469-21
m.fl.

Skäligen misstänkt person	Personnr
Amin, Kojar	19970905-8490

Identifierad	Kontrollsätt	Kommentar
Ja	Känd av polisanställd	

Polisen

Personalia och dagsbotsuppgift

Utskriftsdatum
2022-05-20

Namn			Personnummer
Amin, Kojar			19970905-8490
Tilltalsnamn	Kallas för	Öknamn	Kön
			Man
Födelseförsamling	Födelselän	Födelseort utland	
Gottsunda	Uppsala län		
Medborgarskap	Hemvistland	Telefonnr	
Sverige		0764050366: Mobiltelefon	
Adress		0790212127: Annat telefonnummer Ringer in på	
Solistvägen 6		nummer.	
756 54 Uppsala			
Folkbokföringsort		Senast kontrollerad mot folkbokföring	
Uppsala		2022-04-26	

Föräldrars/Vårdnadshavares namn och adress (beträffande den som inte fyllt 20 år)

Utbildning

Yrke / Titel

Arbetsgivare | Telefonnr

Anställning (nuvarande och tidigare)

Arbetsförhet och hälsotillstånd

Kompletterande uppgifter

Uppgiven inkomst	Bidrag	Hemmavarande barn under 18 år
0	Nej	
Försörjningsplikt		Skulder
nej		0
Förmögenhet		
0		

Kontroll utförd

Taxerad inkomst	Taxeringsår
0	2020
Taxeringskontroll utförd av	Datum
PA Lagerbäck	2020-04-08

Polisen

Bilaga - Skäligen misstänkt

Enhet	Diarienr
Region Mitt, Grova brott 1 PO Gävleborg	5000-K753871-21

Skäligen misstänkt person	Personnr
Dawlatzai, Naser Musa	19980420-8230

Identifierad	Kontrollsätt	Kommentar
Ja	Annat	id av polis uppsala, se K597165-21