Polisen

Protokollbilaga

Arkiv/Åkl. ex

Åklnr
AM-81522-21

Signerat av
Robin Lind

Signerat datum
2022-05-24 17:10

Enhet
Region Nord, Aktionsgrupp 1 Rgn Nord

Handläggare (Protokollförare)
Robin Lind

Datum
2022-03-29

Undersökningsledare
Oskar Edvardsson

Polisens diarienummer
5000-K601538-21

Personer i ärendet

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

Misstänkt (Efternamn och förnamn)	Personnummer
Lanuza, Björn Luis	19850915-7478

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
Mail till häktet Kronoberg	2022-03-30		2022-05-24
Försvarare Andersson, Elsa, förordnad 2021-07-21	2022-03-31		2022-05-24

Underrättelsesätt, försvarare	Resultat av underrättelse mt	Resultat av underrättelse försv
Via post	Erinran, 2022-05-02	Erinran, 2022-05-02

Notering

Innehållsförteckning

Diarienr	Uppgiftstyp	Sida
	Generella dokument Encrochat	
	Polisen - NOA	
5000-K601538-21	PM Encrochat Nationella operativa avdelningen	3
	NOA - Positioneringar i Encrochatmaterial	5
	Lärdomar av Encrochat - NOA Analysprojekt Robinson	7
	Polisen - NFC	
	NFC Förkonfigurerade enheter, Notat 2020:09	41
	NFC Notat komplettering	55
	Franska myndigheter	
	Encrochat, Fransk redogörelse	56
	Generella dokument SKY	
	Övergripande info SKY ECC	62
	Pressmeddelande från Eurojust gällande SKY ECC	63
	NFC SKY	65
	Tolkning av information SKY	79
	Personalia	
	Bilaga skäligen misstänkt, Lanuza, Björn Luis	81
	Personalia, Lanuza, Björn Luis	82

Polisen

PM

Datum
2020-09-17

Diarienr (åberopas)
A526.774/2020

Saknr
403

Polismyndigheten
Nationella operativa avdelningen

EncroChat

Inledning

Sedan april 2020 har svensk polis via Nationella operativa avdelningen (Noa) deltagit i en ”Operational Task Force” 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.

I och med genombrottet tillsatte Europol en Operational Task Force som sedan april 2020 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.

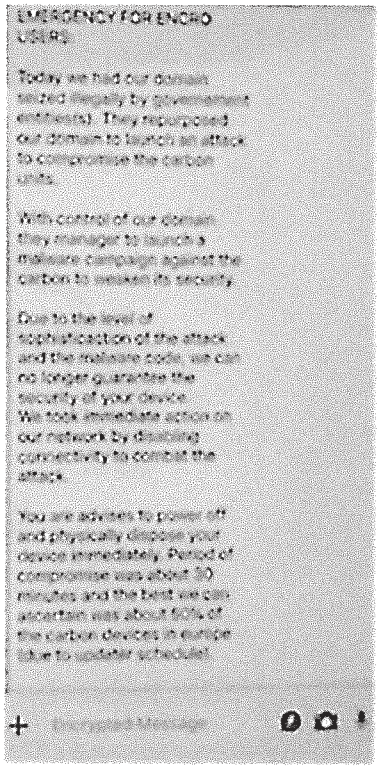
Den information som underrättelseverksamheten har haft och fortfarande har tillgång till omfattar i huvudsak perioden 1 april till 13 juni 2020. Det finns dock i undantagsfall information som härstammar från tider före och efter

dessa datum. Svenska myndigheter har enbart fått använda materialet för att inleda förundersökning och för att på andra sätt förhindra grova brott, inte för andra förundersökningsåtgärder.

Att använda materialet i en förundersökning förutsätter att en europeisk utredningsorder, EIO, utfärdats och skickats via Eurojust. Efter tillstånd av behörig fransk myndighet överlämnas materialet via Eurojust varvid all information delges svensk polis eller annan berörd brottsbekämpande myndighet.

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, Informationstekniksektionen, som i sitt sammanfattande dokument ger en teknisk beskrivning och analys av enheternas och EncroChats funktionaliteter.

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.

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.

Lärdomar av Encrochat

- Analysprojekt Robinson

Nationella operativa avdelningen, Underrättelseenheten

2021-05-10

Polisen

RAPPORTMISSIV

Avdelning/Region	Enhet
Noa	Underrättelseenheten
Diarienummer	**Titel**
A193.902/2021	Lärdomar av Encrochat - Analysprojekt Robinson
Ansvarig chef	**Beställare**
Linda H. Staaf	C Noa
Omfattning	**Produkt**
35	Strategisk rapport

Sammanfattning

I rapporten *Lärdomar av Encrochat - Analysprojekt Robinson* sammanställs den kunskap som genererats till följd av tillgången till kommunikation från den krypterade tjänsten Encrochat. Rapporten beskriver främst den kriminella miljön kring aktörer med strategisk eller organisatorisk roll inom narkotikasmuggling, eftersom det huvudsakligen är sådana aktörer som återfinns i materialet.

Encromaterialet innehåller information om brottsplaner, om kriminella sammanslutningar och om relationer mellan kriminella aktörer. För att omhänderta informationen har underrättelseenheten vid Nationella operativa avdelningen (NOA) och de regionala underrättelseenheterna genomfört ett nationellt analysprojekt. Projektet bedrevs i sju inriktningar: nätverk, våld, narkotika, penningtvätt, vapen och sprängmedel, MC-relaterad brottslighet och otillåten påverkan.

I rapporten redovisas resultaten av vartdera analysprojekt i separata kapitel. Rapportens avslutande kapitel summerar den bild av encroanvändarna som analysarbetet genererat samt redogör för ett antal övergripande samhällssårbarheter som framkommit inom ramen för arbetet.

Produktinformation	Sekretess
Öppen	Ingen

Beslut

☒ Rapporten är fastställd

Stockholm 2021-05-10

Linda H. Staaf, Chef Underrättelseenheten Nationella operativa avdelningen, NOA

Sammanfattning

Encrochat kan närmast beskrivas som en marknadsplats för kriminella som präglas av skiftande kontakter och snabba beslut. Förväntan om att tjänster återbetalas av gentjänster framstår som vägledande för de kontakter som knyts på plattformen, snarare än klart definierade hierarkiska roller eller nätverkstillhörigheter. Samverkan sker såväl inom som mellan identifierade nätverk, samt med personer som verkar sakna grupptillhörighet.

Encrochat-plattformen är till stor del ett sammansatt narkotikanätverk där de flesta når ut brett till personer med hög kriminell kapacitet. Detta medför att få personer på plattformen är oersättliga och det är tveksamt om insatser mot enskilda individer i detta skikt skulle inverka nämnvärt på den totala narkotikainförseln.

Ett högt säkerhetstänk är gemensamt för aktörerna i materialet. Detta bekräftas bland annat av att man genomgående använder sig av yngre personer för att utföra vissa brott och anlitar personer som är okända för polisen till att lagerhålla narkotika, kontanter och vapen, samt för tillgång till fordon för transporter. Aktörerna påstår sig också ha etablerade kontakter med tjänstemän inom bankväsendet, på myndigheter, på företag och med advokater.

Materialet visar på en hög våldsbenägenhet bland aktörerna och en låg tröskel till dödligt våld. Våldet är inte alltid direkt orsakat av narkotikauppgörelser, även om det sker i sociala miljöer som är uppbyggda runt narkotika. Våldet kan drivas av personliga konflikter, hämndspiraler och som strategi för att inte själv angripas först. Det dödliga våldet är ofta anstiftat och utförligt planerat. Tillgången till vapen, ammunition, medhjälpare och utförare är i regel god och utgör inte en begränsande faktor för genomförandet. Drivkraften för unga utförare, som ofta saknar direkt koppling till anstiftaren, kan vara såväl ekonomisk som att stiga i graderna och visa sig pålitlig. Det våld som utförs under perioden är bara en liten andel av alla fall där våld diskuteras och planeras.

Narkotikasmugglingen till Sverige bedrivs i en närmast industriell skala som troligtvis uppnår nivåer om över 100 ton årligen. Att omfattande införsel har kunnat bedrivas samtidigt som nationsgränserna varit stängda bekräftar att legal godstrafik, som varit undantagen restriktioner, används som transportsätt. Pengarna som omsätts och kostnaderna för narkotikainförseln uppnår troligen miljardbelopp årligen. Stora delar av brottspengarna som genereras i Sverige växlas till euro och förs utomlands för återinvestering i nya partier. Valutaväxling är en central funktion i smugglingskedjan.

Tillgången till krypterad kommunikation är avslutningsvis en förutsättning för snabb koordinering av våldsbrott och organisering av storskalig narkotikasmuggling. Kommunikationen påskyndar brottsförlopp och underlättar att knyta kontakter med nödvändig kompetens i brottskedjan, som man annars inte hade haft tillgång till. Även om insatsen mot Encrochat kan ha haft en avskräckande effekt fortgår sannolikt liknande kriminell kommunikation på andra krypterade plattformar.

1 Inledning

Under våren 2020 lyckades franska myndigheter tillsammans med Europol tillgängliggöra innehållet i den krypterade kommunikationstjänsten Encrochat. Svensk polis fick sedermera tillgång till de användarkonton som befann sig i Sverige, eller hade kontakt med användare i Sverige, och kunde i realtid följa kriminella aktörers brottsplaner. I tron om att Encrochat var ett säkert kommunikationsverktyg användes det för att ohämmat diskutera brottsplaner. Detta gav svensk polis ett fördelaktigt operativt läge vilket ledde till ett stort antal ingripanden. Arbetet genomfördes som flera insatser inom ramen för en operation som benämndes Operation Robinson.

Frånsett de rent operativa framgångarna kan materialet också fungera kunskapshöjande. Bland meddelandena finns till exempel detaljerad information om brottsplaner, kriminella sammanslutningar och om relationer som tidigare varit okända för Polismyndigheten. Polisens underrättelsetjänst har i och med tillgången till materialet haft möjlighet att höja kunskapsläget avseende en rad brottsområden och dess modus samt identifiera och kartlägga tidigare okända kriminella nätverk och tongivande aktörer.

I syfte att säkerställa att de kunskaper som genererades i och med tillgången till materialet tas tillvara, och för att skapa mervärde kring informationen, genomförde underrättelseenheten vid Nationella operativa avdelningen (NOA) och de regionala underrättelseenheterna ett nationellt analysprojekt. Projektet bedrevs i följande sju inriktningar: nätverk, våld, narkotika, penningtvätt, vapen och sprängmedel, MC-relaterad brottslighet och otillåten påverkan. Analysprojektet avrapporteras i sin helhet i föreliggande rapport.

1.1 Metod

Under hösten 2020 genomfördes en systematisk genomläsning och kodning av materialet. Denna bearbetning låg till grund för den analys som sedan följde. Utöver det har en kvalitativ informationsinhämtning skett genom enkäter där projektets deltagare har svarat på frågor om hur de, med hänsyn till sin tidigare sakkunskap inom respektive brottsområde, tolkat det material som de tagit del av. I syfte att kvalitetssäkra processen, från bearbetning till analys, bildades en styrgrupp som löpande har följt upp arbetet.

1.2 Begränsningar

Materialet är begränsat både tidsmässigt (våren 2020), rumsligt (en kommunikationstjänst) och avseende brottsområde (främst organisering av narkotikasmuggling). Detta innebär att Encrochat inte ger en inblick i övrig organiserad brottslighet, såsom exempelvis människosmuggling, internetrelaterade sexualbrott mot barn eller terrorism. När det gäller den tidsmässiga avgränsningen är det värt att ha i åtanke att projektet pågick under utbrottet av Covid 19-pandemin, vilken medförde en rad åtgärder som i många avseenden tvingade Encrochat-användarna till anpassning. Bland annat reste många av de utlandsbaserade kriminella tillbaka till Sverige och möjligheten att bedriva narkotikahandel påverkades av utökade gränskontroller, karantänsregler med mera. Därtill pågick den särskilda händelsen Rimfrost på olika platser i Sverige som kan ha tvingat många kriminella till en anpassning därefter. Slutligen ska det understrykas att denna rapport i huvudsak är baserad på en källa med de begränsningar det innebär.

2 Nätverk

2.1 Inledning

Encronätverket är en del av en sammankopplad miljö som präglas av narkotikadistributörer på hög eller medelhög nivå. De verkar i vad som kan beskrivas som en tillfällesekonomi där de i högt tempo gör affärer med andra distributörer och ständigt letar efter nya brottstillfällen. I en sådan sammankopplad miljö finns det många användare som har lång räckvidd och som lätt kan nå ut till personer med hög kriminell kapacitet. Användarna har ofta flera parallella kontakter med samma sorts kompetens och flera olika vägar att nå ut i nätverket, vilket innebär att få personer är strategiska i bemärkelsen att de är oersättliga.

Det finns behov av snabba beslut och kontaktvägar, även över längre geografiska avstånd, vilket gör att tillgången till krypterade kommunikationskanaler är avgörande. Många använder flera krypterade kommunikationstjänster parallellt, vilket innebär att materialet endast ger oss viss insyn i nätverken och samverkan i miljön. Att det är en begränsad grupp som använt Encrochat, främst aktörer med strategisk eller organisatorisk förmåga – så kallade a- och b-aktörer[1], innebär att vi inte ser de lägre skikten i aktörernas kriminella nätverk. I stort sett alla användare är involverade i narkotikabrottslighet, bland de fåtal personer som inte ägnar sig åt narkotikahandel dominerar penningtvätt och utbyte av finansiell kompetens. Dock hanterar denna verksamhet oftast pengar som används för, eller genereras av, narkotikabrottslighet.

De analyser som genomförts i syfte att förtydliga hur relationerna mellan de olika användarna ser ut bygger dels på kvantitativa mått och beräkningar av användarnas interaktioner och kommunikationsmönster, dels på kvalitativa beskrivningar och regionala fördjupningsstudier[2].

2.2 Relationer inom den organiserade brottsligheten

Den främsta slutsatsen som kunde dras i och med nätverksanalysen var att de personer som använder Encrochat är tätt sammankopplade och merparten av alla användare ingår i ett stort nätverkselement. På åtta steg nås samtliga användare i nätverket, och om man utgår från personer som befinner sig nära mitten, det vill säga personer med många kontaktytor, nås i genomsnitt knappt 10 procent av alla användare på två steg och knappt hälften på tre steg.[3] Detta innebär att kommunikationen i nätverket kan ta flera olika

1 A-aktör: Strategisk förmåga, kan agera mellan tillgång och efterfrågan på kriminella varor och tjänster. B-aktör: Hanterar och bevakar kriminella intressen i en lokalt avgränsad marknad, är mer av en utförare.

2 Alla deltagare i analysprojektet har besvarat en enkät som berör nätverksanalysens teman. Deltagare från regionerna Syd och Väst, Stockholm, Mitt och Öst har gjort egna fördjupningar.

3 Den höga graden av sammankoppling visar sig också genom förekomsten av trianglar. Trianglar är ett centralitetsmått som anger hur tätt ett nätverk är. I ett tätt nätverk har alla aktörer kontakt med varandra. En person som har två kontakter ingår i en triangel om hans kontakter även har kontakt med varandra. Generellt sett är denna sammankoppling hög i materialet.

vägar mellan användarna och att det är få personer som är oumbärliga för att kommunikationen ska flöda.[4]

Det som styr vilka aktörer som samverkar, som har relationer med varandra och graden av lojalitet är möjligheten att göra affärer. Aktörerna kan beskrivas som opportunister och kriminella entreprenörer, som handlar ad-hoc där utbud och efterfrågan är det mest styrande för vilka relationer som uppstår. Nya kontakter knyts enkelt genom referenser från gemensamma bekanta och när en person har behov av till exempel specifik kunskap eller en illegal vara vänder sig denne snarare direkt till en person som besitter detta än att låta sig avgränsas till mer etablerade relationer. Graden av tillit mellan encroanvändarna bedöms generellt som hög.

När det gäller huruvida aktörerna kan kopplas till kända nätverk eller andra typer av grupptillhörigheter så är det något som sällan framgår av materialet[5]. Hierarkier och roller framträder förvisso i vissa fall, där vissa aktörer lägger ut uppdrag och andra aktörer tar emot och utför dessa. Region Stockholm har till exempel i sin analys identifierat ett nätverk som är strikt hierarkiskt och som har en tydlig ledare. Trots detta finns dock inslag av samverkan mellan aktörer i nätverket utan involvering av personer högre upp i hierarkin och direkt samverkan mellan personer i nätverket med aktörer utanför. Den samverkan som sker verkar alltså inte behöva sanktioneras eller godkännas av nätverkets ledare och även denna brottslighet framstår som projektbaserad och tillfällig. Dock finns det gränser och man samverkar inte med aktörer som upplevs som direkta rivaler eller där det finns pågående konflikter. Sammantaget framstår det enligt materialet som att den kriminella samverkan är mer gränslös och utbredd än vad som tidigare var känt. Utifrån konversationerna framträder att överenskommelser görs utifrån en förväntan om ömsesidighet och att tjänster återbetalas av gentjänster, snarare än utifrån klart definierade hierarkiska roller. Aktörerna drar i vissa fall fördel av att tillhöra en kriminell gruppering, även om en stor del av kontakterna på Encrochat sker som en del av kriminellt entreprenörskap.

2.2.1 Användarnas brottslighet

Narkotikabrottslighet är det mest förekommande brottsområdet i materialet. Det är bara en minoritet av användarna som inte ägnar sig åt narkotikahandel (runt 10 procent av samtliga konton). Den vanligaste rollen som användarna har är att de fungerar som nationella organisatörer[6]. De flesta hanterar medelstora till relativt stora partier narkotika och säljer dem vidare till andra leverantörer inom landet. Kommunikationen förs i ett högt tempo och kontaktnäten är breda.

De aktörer som inte är involverade i narkotikahandel ägnar sig främst åt penningtvätt, följt av våld och vapenbrott. Därefter finns enstaka personer som ägnar sig åt kombinat-

4 Framträder även i den regionala analysen av Region Mitt samt i analyssamarbetet mellan regionerna Syd och Väst, som fokuserade på kontakter mellan regionerna Syd och Väst.

5 Då grupptillhörigheter inte framträtt som styrande, utan aktörerna till stor del representerar sig själva, så har det inte varit motiverat att analysera materialet utifrån exempelvis specifika grupperingar eller släktbaserade nätverk.

6 Person som organiserar narkotikahandel inom landet men inte själv står för insmuggling till landet.

ioner av bedrägerier, otillåten påverkan, företag i brottslig verksamhet och penningtvätt. Det finns även ofta en överlappning mellan narkotika och vapen, våld eller penningtvätt.

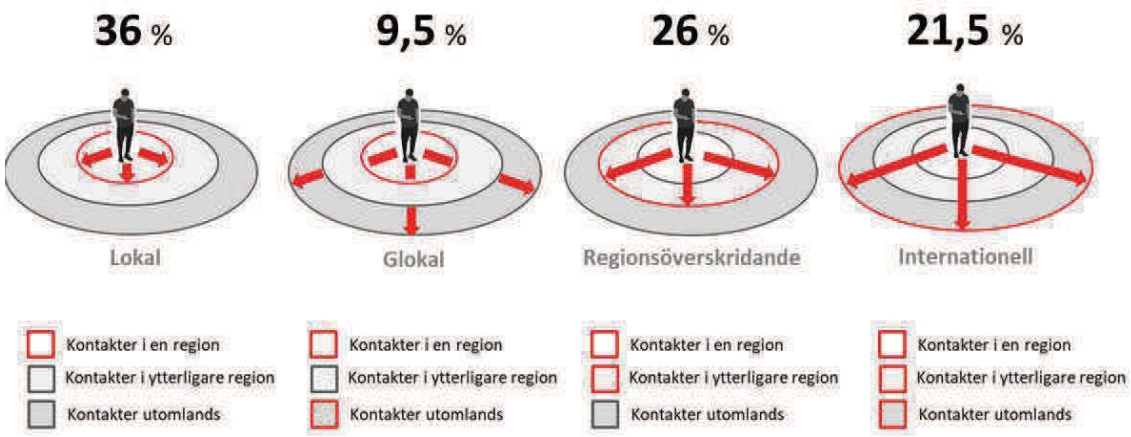
Graden av struktur och specialisering följer i flera fall storskaligheten i aktörernas brottslighet och bedöms i regel som högre för personer som samverkar med internationella kontakter, smugglare och transportörer. När det gäller aktörer som har en tydligare lokal förankring är intrycket att dessa i större utsträckning agerar tillfällesstyrt och ad-hoc.

2.2.2 Nationell och internationell samverkan och relationer

Ungefär 40 procent av användarna befann sig i Sverige under den aktuella tidsperioden och knappt 15 procent befann sig utomlands. För övriga saknas information. Majoriteten av personerna som befann sig i Sverige uppehöll sig i Stockholm (knappt 40 procent) följt av Väst och Syd (drygt 25 procent vardera). De som befann sig utomlands vistades framför allt i Nederländerna och Spanien. Generellt sett är de flesta användarna tydligt förankrade i en viss polisregion, men de har ofta någon regionsöverskridande kontakt (vilket cirka hälften av användarna har). Det är ovanligare att användarna har internationella kontaktnät, men drygt 30 procent har åtminstone en kontakt som befann sig i ett annat land under perioden.

Det kan också konstateras att storstadsaktörerna rent fysiskt är relativt tydligt geografiskt förankrade och att resor med Encrochat-telefonen är sällsynta. Aktörernas interregionala nätverk är omfattande och dessa verkar präglas av samarbete och ömsesidig ekonomisk vinning snarare än av konkurrens. Detta kan möjligen bero på att aktörerna inte konkurrerar om samma lokala marknad.

De olika användarnas internationella och regionsöverskridande kontaktnät kan beskrivas i fyra olika kategorier (se bild nedan). Den största gruppen består av användare som endast har kontakter i en region, följt av användare som har kontakter i flera regioner men som, åtminstone på Encrochat, saknar kontakter med aktörer i andra länder. Därefter följer användare som har såväl regionsöverskridande som internationella kontakter. Den minsta kategorin användare utgörs av personer som endast kommunicerar med användare i en region i Sverige men som samtidigt har kontakter som befinner sig utomlands. Utöver dessa finns en mindre grupp (cirka sju procent) som endast har kontakter med användare utan känd geografisk tillhörighet.



Figur 1. Olika typer av geografiska samverkansprofiler. (Sju procent av aktörerna gick inte att bedöma, eftersom de huvudsakligen har kontakter med användare som saknar känd uppkoppling)

Användarna i respektive kategori skiljer sig delvis från varandra. Generellt sett kan man säga att de med internationella kontakter (de glokala[7] och de internationella) sticker ut i volymen meddelanden och kontaktantal (degree[8]). De har också högre betweenness[9] än de andra grupperna, sannolikt för att de internationella aktörerna ökar räckvidden i en persons kontaktnät. De har även högst antal och andel trianglar. De som har breda kontaktnät inom Sverige (de regionsöverskridende och de internationella) har som regel en högre andel a-aktörer i sina kontaktnät men även en högre andel användare som bedöms vara våldsanstiftare och vapenförsäljare.

De lokala har ofta mindre kontaktnät, och de har som regel färre kontakter med a-aktörer eller användare som ägnar sig åt mer avancerad brottslighet. Det är dock viktigt att notera att de flesta användarna, oavsett kategori, aldrig har långa sociala avstånd till personer som befinner sig utomlands under perioden eller som är involverade i mer avancerad kriminalitet. Till exempel har de flesta mer än en kontakt som i sin tur kommunicerar med någon som befinner sig utomlands.

2.2.2.1 Skillnader mellan storstadsregionerna

Det finns vissa skillnader när man jämför storstadsregionerna med varandra. Användarna i region Syd har oftare internationella kontakter och kontakter i andra regioner jämfört med Stockholm och Väst. Väst har lägst andel användare med internationella kontakter. De har också en högre andel trianglar i sina kontaktnät än övriga storstadsregioner, vilket innebär att de befinner sig i mer tätt knutna miljöer. Samtidigt har en relativt hög andel av dem kontakt med någon användare i en annan region. Stockholmsaktörerna kan sägas ha en mer glokal profil. Om man tittar på kommunikationsflödet mellan

7 Glokal: aktören har både kontakter i regionen (lokal) och utomlands (global). Se figur 1.

8 Centralitetsmått som anger hur många kontakter en aktör har i nätverket. En aktör med hög degree knyter samman många aktörer i sina direkta kontakter.

9 Centralitetsmått som identifierar aktörer som är centrala i nätverket genom att de knyter ihop stora delar av nätverket, genom sina direkta och indirekta kontakter. De behöver inte ha en hög degree själva för att få en hög betweenness-centralitet.

storstadsregionerna kan man konstarera att det är relativt jämt fördelat. Användarna i Stockholm kommunicerar med ungefär lika många i Syd som i Väst, användarna i Väst kommunicerar med ungefär lika många i Stockholm, som i Syd, och så vidare.

2.2.2.2 Internationella flöden

Informationsflödet mellan konton i Sverige och andra länder följer i stort sett underrättelsebilden som svensk polis haft sedan tidigare över internationell samverkan. Flödet är, som tidigare nämnts, störst till och från Spanien följt av Nederländerna.

Värt att notera är också att spanienaktörerna tycks ha bredare förgreningar i Sverige än vad de som befinner sig i Nederländerna har. Från Spanien kommunicerar 82 personer med 222 i Sverige. Från Nederländerna är förhållandet närmre 1:1. Aktörerna i Spanien har också kontakter med personer i flest regioner i Sverige. Förutom storstadsregionerna kommunicerar de med aktörer i Öst, Mitt och Bergslagen. Spanienaktörerna har flest kontakter i Stockholm, följt av region Syd. Syd har överlägset flest av Danmarkskontakterna. Väst har flest från Norge och Storbritannien men det rör sig om ett lågt antal användare. De flesta utlandskontakterna är svenskar som befann sig utomlands under perioden. Endast en mindre del tycks vara utländska medborgare utan tidigare koppling till Sverige.

Det mesta talar för att användare i Sverige sällan har direktaccess till utländska kriminella nätverk, utan går via en svensk kontakt som befinner sig i ett annat land. Eftersom svensk polis endast har fått ta del av konversationer som gick in och ut från Sverige, har vi ingen fullständig bild över de utlandsbosatta svenskarnas internationella nätverk.

2.2.3 Aktörer

Som tidigare beskrivits utgörs Encronätverket av ett stort antal användare som har lång räckvidd och som lätt kan nå ut till personer med stor kriminell kapacitet. En stor andel av alla användare har bedömts vara a-aktörer och det finns en stor redundans i nätverket. Detta medför att få personer är oersättliga. Undantaget är eventuellt de fåtal personer som har finansiell spetskompetens.

De övriga analysinriktningarna som beskrivs i rapportens inledning har gått igenom materialet utifrån specifika brottsområden, och identifierat ungefär fem användare per inriktning som de bedömt vara särskilt tongivande genom att de har en mycket omfattande och avancerad brottslighet.

De tongivande aktörerna har ofta kontakt med varandra och få är helt specialiserade på sina brottsområden. Ur ett nätverksperspektiv utmärker sig de flesta av aktörerna på flera olika sätt, till exempel genom att ha högt informationsflöde, breda kontaktnät och en ovanligt hög andel A-aktörer i sina kontaktnät. Det framstår också som att det finns vissa skillnader mellan aktörerna, till exempel har de som är tongivande inom narkotika något högre informationsflöde, fler kontakter och utlandskontakter, än vad de användare som är tongivande inom andra brottsområden har. De agerar i en internationell miljö vilket också medför att de får kortare avstånd mellan Encronätverkets kanter och oftare har en något högre betweenness.

De tongivande personerna i de olika brottsinriktningarna har också ofta många kontakter med andra personer i de högre skikten inom samma brottsområde[10]. Men även om det finns vissa nyansskillnader mellan grupperna, utmärker sig de flesta genom att de avviker från övriga användare när det gäller deras utfall på olika nätverksmått[11]. Det är ovanligt att tongivande användare håller en lägre profil vilket medför att en nätverksanalys ger förutsättningar för att identifiera dessa.

10 Innebär att tongivande användare i narkotika har en hög andel internationella organisatörer i sitt egonätverk, och tongivande våldsverkare har en hög andel våldsanstiftare i sina.

11 Några av de aspekter vi beaktade var: degree, betweenness, trianglar, utlandskontakter, kontakter i antal regioner, kontakter med a-aktörer, kontakter med internationella narkotikaaktörer, kontakter med anstiftare i våld, kontakter med tongivande vapenaktörer.

3 Våld

3.1 Inledning

Svensk polis ingrep under våren 2020 mot cirka tio långt framskridna mordplaner baserat på informationen från Encrochat. Detta är dock bara en liten andel av alla fall i materialet där våld diskuteras och planeras. Språkbruket är ofta rått och våldsamt och många tycks ha ett behov av att uppvisa en aggressiv framtoning. Många gånger är det dessutom slumpmässiga omständigheter som avgör om våldsdåd genomförs, skjuts på framtiden eller avbryts. Man kan därför säga att våldet som faktiskt utförs bara är toppen av ett isberg av potentiella våldsbrott.

Encrochat har som bekant företrädelsevis använts av personer som har centrala roller i sina respektive brottsområden. Våldsaktörerna som finns i materialet innehar framförallt roller som anstiftare och möjliggörare. Deras förmåga och behov att planera och organisera våldsupplägg skiftar. Vissa planerar på detaljnivå medan andra agerar på ett sätt som för en utomstående närmast kan upplevas slentrianmässigt. Personerna som åtar sig att utföra våldsdåd befinner sig ofta något led från anstiftarna.

Distanseringen mellan anstiftare och utförare medförde inte bara en trolig mental avskärmning hos anstiftaren utan även en polisiär utmaning i att dels följa den faktiska händelsekedjan, dels lagföra de personer som anstiftat brottet.

Detta avsnitt är baserat på fallstudier av tretton separata våldsupplägg där hela eller delar av planeringen avhandlades på Encrochat.

3.2 Våldsupplägg, roller och drivkrafter

I materialet förekommer dels våld som kan kopplas till tidigare kända långvariga konflikter, dels mer hastigt uppkommet våld. I de långvariga konflikterna är det endast i liten utsträckning som våldsbrotten bedöms ha direktkoppling till ursprungsmotiven. Konflikterna har i större utsträckning övergått till långvariga våldsspiraler där tidigare våldsbrott föder fram nya och där ett hämnd- och vedergällningsmotiv tagit överhanden och driver våldet framåt.

3.2.1 Planeringsfas

3.2.1.1 Anstiftare och medhjälpare

I de studerade våldsfallen är våldet i huvudsak beställt, dvs. det är någon annan än den med den ursprungliga avsikten som i slutändan genomför brottet. Anstiftaren bakom brottet kan för en utomstående närmast liknas vid en projektledare som tillsammans med ett antal medhjälpare samlar in relevant information och vidtar praktiska åtgärder för att underlätta genomförandet av brottet. Även om anstiftaren själv kan hjälpa till med en del praktiska detaljer så har denne i regel en mer samordnande funktion. Hur stor del anstiftaren tar i planeringsarbetet varierar från fall till fall – i vissa fall är denne mycket aktiv och deltagande medan det också finns exempel på konstellationer som erbjuder en helhetslösning – de åtar sig ett mordkontrakt, gör relevanta förberedelser och utför brottet vilket också kräver ett mindre engagemang från beställaren.

Medhjälparna är oftast personer som befinner sig i anstiftarens närhet och bedöms befinna sig längre ner i den kriminella hierarkin. Det är möjligt att dessa personer ibland inte är helt insatta i vad deras tilldelade uppdrag syftar till. Medhjälparnas uppgifter kan t.ex. handla om att ordna vapen, flyktbil, gömställe och att genomföra informationsinsamling om det tilltänkta brottsoffrets förehavanden.

I de flesta fallen har anstiftaren sedan tidigare en förhållandevis god uppfattning om det tilltänkta offrets leverne men försöker komplettera detta med ytterligare information för att skapa så goda förutsättningar för genomförandet som möjligt. Informationsinhämtningen sker relativt brett men med förhållandevis enkla medel. Det kan t.ex. handla om regelrätt spaning, internetsökningar, utfrågning av mänskliga källor och teknisk inhämtning genom t.ex. att fästa en GPS-puck på motståndarens fordon.

Att ordna med vapen framstår som ett av de enklare momenten under planeringsfasen, varför vapentillgången i de aktuella miljöerna bedöms som god. I vissa fall diskuteras vapenfrågan knappt, vilket kan tolkas som att vapen redan finns tillgängliga i den aktuella sfären. I andra fall är vapen ett eller två steg bort och införskaffas utan större svårigheter.

Att få tag på ammunition till vapnet tar något längre tid men framstår på det stora hela inte som en begränsande faktor för våldet. När det gäller aktörernas kunskap kring vapen och ammunition framträder i en del fall osäkerhet avseende vilken typ av ammunition som passar vilken typ av vapen samt huruvida vapnet är funktionsdugligt eller inte.

Vidare är det tillsynes relativt ovanligt att anstiftaren fysiskt träffar sina medhjälpare. Om det uppstår ett behov av t.ex. ett fysiskt överlämnande sker detta oftast via ombud. Att på behörigt avstånd kunna beställa, planera och samordna grovt våld har möjligen inneburit att det är lättare att ta beslut om liv eller död. Att kunna kommunicera på ett upplevt tillförlitligt sätt har dessutom sannolikt ökat effektiviteten i såväl planering som genomförande.

3.2.1.2 Anstiftare och utförare

Som nämnt i nätverksavsnittet knyts nya kontakter enkelt över Encrochat och bara det faktum att en person innehar en Encro-enhet tycks ofta räcka som bevis på att personen går att lita på.

Fördelningen mellan att en aktör vänder sig till en utförare från det egna kontaktnätet eller anlitar en extern utförare är jämnt i det analyserade materialet. Underlaget visar vidare att det är förhållandevis enkelt att hitta och anlita personer som är villiga att utföra våld oavsett om det rör sig om sprängdåd, skadeskjutningar eller mord, däremot kan det vara desto svårare att hitta en utförare som är pålitlig. Det finns exempel på när attentat misslyckas och när skyttar får kalla fötter och söker anledningar att dra sig ur. En tänkbar förklaring till detta kan vara att man i ganska stor utsträckning är benägen att använda sig av yngre personer som rimligtvis inte har någon större erfarenhet av att befinna sig i en skarp våldssituation.

När en utförare rekryteras i det egna ledet kan detta exempelvis bero på att det är lättare att styra en person med koppling till det egna nätverket. Den största orsaken torde emellertid ligga i att det inom vissa grupperingar redan finns utarbetade strategier och en konstant hög förmåga att agera med dödligt våld.

I de fall en utförare eftersöks utanför det egna nätverket är det vanligt att anstiftaren frågar sina tidigare kontakter om de vet någon som kan utföra det aktuella brottet. I vissa fall får anstiftaren på så vis direktkontakt med en utförare, men det är även vanligt att den tillfrågade kontakten agerar mellanhand mellan anstiftaren och utföraren och att dessa inte har någon direktkontakt med varandra. Syftet med detta torde vara att försvåra lagföring genom att skapa distans mellan anstiftare och utförare.

När en extern aktör eftersöks för att antingen genomföra en skjutning eller för att i sin tur rekrytera en utförare är det vanligt att hela våldsupplägget saluförs som en ”paketlösning” där alla praktiska detaljer som t.ex. flyktbil, gömställe och vapen redan är omhändertagna och det enda som kvarstår är en person som är villig att genomföra brottet. I ett sådant upplägg är ofta även en så kallad ”goare”[12] inkluderad. Genom den vanliga förekomsten av ”goare” framträder dessutom en bild av föränderliga lojaliteter och att det i de aktuella miljöerna sannolikt är svårt att avgöra vem som står på vilken sida.

Ersättningen för ett mord varierar från mellan 100 000 kr till 1 000 000 kr beroende på anstiftarens ekonomiska förutsättningar, vem det tilltänkta offret är och vilken erfarenhet utföraren har. Det är t.ex. billigare att anlita en ung person utan erfarenhet än vice versa. Utöver ekonomiska incitament som drivkraft för att utföra ett våldsbrott förekommer det även hämndmotiv. Det är även förekommande att unga personer åtar sig morduppdrag utan krav på ekonomisk motprestation i syfte att visa sig pålitliga och för att stiga i graderna.

[12] Goare: En person som ska lura brottsoffret till en lämplig plats att genomföra mordet på. Ofta bekant eller närstående till det tilltänkta brottsoffret. Drivkraften för en goare är ofta någon sorts hämndmotiv och/eller att man har dubbla lojaliteter sedan tidigare. Det finns ett exempel där en person blivit misshandlad och förnedrad och erbjudit att lura offret som ett led i sin egen hämnd.

I samband med att den ekonomiska ersättningen förhandlas finns det också exempel på diskussioner om vad som ska gälla vid eventuella misslyckanden, t.ex. att det tilltänkta offret skadas men inte avlider.

I samband med diskussioner om ersättning utifrån olika scenarion förekommer det också att anstiftare kommer med specifika önskemål om själva utförandet. Det kan t.ex. handla om att anstiftaren vill att brottsoffret ska skjutas i huvudet eller att ett stort antal kulor ska avfyras mot kroppen för att säkerställa att personen dött.

3.2.2 Genomförande- och efterfas

När ett planerat våldsdåd övergår från planeringsfas till ett genomförande beror detta i huvudsak på att ett tillfälle att utföra brottet uppstår. Orsakerna till att våldsplaner avbryts utan polisiär inblandning kan i många fall tillskrivas slumpen. I vissa fall rinner planerna ut i sanden, utföraren ångrar sig eller så kan t.ex. anstiftaren övertalas om att brottet av olika anledningar inte bör genomföras. Faktisk eller inbillad polisiär närvaro försvårade inte sällan både planering och genomförande. Överlag fanns det en stor känslighet för ryktesspridning och en benägenhet att agera på obekräftad information.

Den tydligaste indikatorn i materialet på att ett våldsbrott är nära förestående är att detta antingen skrivs ut i klartext eller att det framgår av sammahanget. Därtill tenderar mängden in- och utgående trafik på anstiftarens konto öka två dagar innan genomförandet och på själva genomförandedagen. Av fyra fullbordade våldshändelser (två mord, ett mordförsök och en allmänfarlig ödeläggelse) är trafikökningen mellan 28 % och 464 %.

Under genomförandet är det vanligt att anstiftaren kontinuerligt får information om t.ex. skadeläge och hur genomförandet fortlöper. Det är även förekommande att anstiftaren själv anskaffar dylik information genom t.ex. nyhetsrapportering och genom en promenad förbi brottsplatsen.

Efter genomförandet förekommer också att bilder på brottsoffret sprids samtidigt som hån och nedsättande kommentarer uttrycks. Därefter övergår de inblandade aktörernas konversationer förhållandevis snabbt till någon form av normalläge vilket för de flesta av aktörerna innebär diskussioner om narkotikauppgörelser och till viss del även sociala konversationer.

I materialet finns också exempel på när ett mord misslyckas och brottsoffret överlever. Konversationerna övergår i samband med detta relativt skyndsamt över till något som närmast kan liknas vid krishantering. De inblandade aktörerna diskuterar exempelvis hur de ska skydda sig mot eventuella motangrepp, hur evakuering av familjemedlemmar ska gå till samt planer för att ta ytterligare motståndare av daga i ett förebyggande syfte.

3.3 Avslutande iakttagelser

En stor del av våldsbrotten som planeras på Encrochat är anstiftade och i många fall också välplanerade. Givet att den genomsnittliga användaren har en hög kriminell förmåga är det inte konstigt att detta också avspeglar sig i samband med att våldsbrott planeras. Det situationella och mer händelsestyrda våldet bland kriminella med en generellt sett lägre förmåga har sannolikt avhandlats på Encrochat i en mindre omfattning. Våldet såsom det framgår utifrån detta material är sannolikt mer välplanerat än i andra sammanhang.

Den bristande respekten för människoliv, likgiltigheten inför risken att tredje man ska drabbas och det närmast rutinmässiga och mekaniska sättet att ta beslut om liv eller död är dock anmärkningsvärd. Våldet framstår som en integrerad del av många av de inblandade aktörernas livsstil. Detta i kombination med en mycket rörlig och riskpräglad hantering av narkotika och pengar gör att den latenta risken för våld i kriminella miljöer är stor. Den studerade miljön verkar också präglas av ett starkt heders- och vedergällningspräglat förhållningssätt vilket i sin tur riskerar att skapa utdragna och eskalerande konflikter.

4 Narkotika

4.1 Inledning

Avsikten i analysprojektet med inriktning på narkotika är att analysera den svenska narkotikamarknaden och dra generella slutsatser om modus och omfattning kring narkotikasmugglingen till Sverige utifrån materialet i Encrochat.

De aktörer som bedöms som internationella organisatörer av narkotikasmuggling har utifrån materialet kapacitetsbedömts. Detta har gjorts bland annat baserat på den mängd narkotika de bedöms organisera smuggling av under den aktuella perioden. Därefter har en fördjupning genomförts av de 84 aktörer som bedömts vara de mest centrala. Urvalet har gjorts efter en kvalitativ genomgång av samtliga aktörer som initialt bedömts vara internationella organisatörer.

4.1.1 De internationella narkotikaorganisatörerna

De 84 mest centrala aktörerna i materialet smugglar och distribuerar främst hasch, marijuana, kokain och amfetamin, till den svenska narkotikamarknaden. Den narkotika som de internationella aktörerna hanterar fördelas på hasch 52 procent, marijuana 22 procent, kokain 12 procent, amfetamin 11 procent och övrigt 3 procent. Samtliga aktörer är män, främst i åldersspannet 30-39 år. Som beskrivs i kapitel 2 (nätverk) är majoriteten placerade i Stockholm, Malmö och Göteborg, samt utomlands på strategiska platser i produktions- och transitländerna Spanien och Nederländerna.

Relativt många internationella organisatörer befinner sig i Spanien, där majoriteten bedöms vara bosatta, helt eller delvis, på den spanska solkusten. Dessa aktörer har direktkontakt med producenter och kriminella nätverk som i sin tur har direktkontakt med producenter av narkotikan. Bedömningen är att narkotikan köps direkt av producenterna eller indirekt via de kriminella nätverken som agerar grossister åt producenterna. Ett flertal internationella aktörer är själva producenter av narkotikan. I exempelvis Spanien producerar dessa aktörer marijuana i industriell skala avsett för den svenska narkotikamarknaden. I de allra flesta fall använder de internationella aktörerna sig av kontanter som betalningsmedel vid narkotikaaffärer. Det förekommer även att de använder sig av bitcoin, banköverföringar, hawala[13], växlare, faktura, paypal, klockor och guld.

4.1.2 Producentländer, transiteringsvägar och distribution i Sverige

Den narkotika som de internationella aktörerna smugglar till Sverige produceras i ett flertal länder och världsdelar. Det smugglade haschet bedöms främst vara producerat i Marocko, och i mindre omfattning i Libanon. Det smugglade kokainet bedöms i huvudsak produceras i Colombia, Bolivia och Peru. Den smugglade marijuanan bedöms framför allt vara producerad i Spanien, men även i Nederländerna, och i mindre omfattning i Albanien. Det smugglade amfetaminet bedöms främst vara producerat i Nederländerna, och i mindre omfattning i Belgien och Polen.

13 Hawala kan beskrivas som ett informellt penninngöverföringssystem. Betalningsöverföringarna genomförs via, i huvudsak löst sammansatta informella nätverk och utan att pengar direkt överförs fysiskt eller elektroniskt. Elektroniska överföringar sker dock i efterhand, oftast i klumpsummor för att reglera skuld/fordran hawalaagenterna emellan.

Narkotikan transiterar genom ett flera länder på vägen till den svenska narkotikamarknaden. Hasch från Marocko bedöms i huvudsak transporteras genom Spanien, Frankrike, Nederländerna, Tyskland och Danmark. Kokain från Sydamerika bedöms främst transitera genom Nederländerna, Tyskland och Danmark. Marijuana bedöms oftast tas in genom Frankrike, Nederländerna, Tyskland och Danmark och amfetamin genom Tyskland och Danmark.

De internationella aktörerna smugglar sedan narkotikan till Sverige främst via Skåne, där Öresundsbron mellan Danmark och Sverige bedöms som den mest frekvent förekommande gränspassagen. Trafikflödet över Öresundsbron är omfattande och det faktum att de internationella aktörerna brukar detta flöde indikerar att de drar nytta av såväl det höga tempot som volymerna av fordon i syfte att reducera risken för upptäckt. Frekvent smuggling sker även via gränsövergångarna i Helsingborg och Trelleborg och i vissa fall sker smuggling via gränsövergångarna i Göteborg och Stockholm. Generellt sett finns det i de internationella aktörernas konversationer relativt lite information om narkotika som smugglas via Sverige och sedan vidare till andra länder. Den transittrafik som förekommer i materialet går till Norge, Danmark och Finland, där aktörer i Norge är de vanligaste mottagarna av narkotikan.

Narkotikan smugglas i regel till Sverige med vägtransport, främst i lastbil men smuggling sker även med personbil. De internationella aktörerna använder sig bland annat av dolda specialtillverkade lönnutrymmen i fordonen, och transporterna sker ofta inom ramen för företagsverksamhet där narkotikan dolts i legal last. De internationella aktörerna smugglar även narkotikan i post- och kurirflödet, om än i något mindre omfattning.

Det förekommer att narkotikapartierna är försäkrade så att första ledets mottagare i Sverige ersätts med ett nytt parti eller kompenseras på annat sätt vid eventuellt beslag av tullen i gränsövergången.

4.1.3 Storstäderna är de huvudsakliga mottagardestinationerna av narkotikan

Stockholm, Malmö och Göteborg är de huvudsakliga mottagardestinationerna för den narkotika som förs in i Sverige[14]. I vissa fall är fler än en stad slutdestination av det smugglade narkotikapartiet, i andra fall är endast en stad mottagare. Det insmugglade narkotikapartiet styckas därefter upp i mindre partier som distribueras till olika mottagare i Sverige. Majoriteten av de internationella aktörerna distribuerar narkotikan via egna organisationer.

Det finns likheter i hanteringen av större narkotikapartier oavsett var i Sverige de hanteras. Ett genomgående tema är att de internationella organisatörerna inte vill lagerhålla de importerade partierna under någon längre tid utan vill distribuera ut dessa så snabbt som möjligt. Initialt kommer huvudmännen överens på Encrochat om vad som ska överlåtas och priset för detta samt tid och plats för överlåtelse och betalning. Överlåtelse och betalning sker ofta vid olika tillfällen och platser för att sprida riskerna. Huvudmännen informerar därefter varandra om signalement på personerna som levererar ut partierna (så kallade löpare eller springisar) och eventuella fordon. Man har även en överens-

14 Även andra större orter är mottagare av smugglade partier narkotika, exempelvis Helsingborg, Uppsala, Linköping, Örebro, Karlstad, Växjö, Eskilstuna och Västerås.

kommen kod som ska sägas av överlåtaren och mottagaren för att bekräfta att man verkligen har rätt person framför sig vid överlåtelsetillfället. Det finns i Encrochat väldigt få meddelanden mellan huvudman och utläggaren vilket tyder på att dessa kommuniceras på annat sätt.

Det har varit svårt att klarlägga vad som sker vid själva uppdelnings- och distributionstillfället av de stora partierna. Utifrån Encrochat går det att följa narkotikapartiets väg från inköp på grossistnivå fram tills partiet är på väg in till Sverige. Dock saknas kommunikation kring partiets sista färdväg och slutdestination. Det verkar som att huvudmännen undviker att vara på plats vid dessa tillfällen. Troligen tas narkotikan emot av personer med lägre status i den kriminella kontexten. Koordinering kring detta sker möjligen genom andra kommunikationsmedel som personer lägre ner i smugglingskedjan har tillgång till.

4.2 Hur mycket narkotika smugglas in i Sverige?

Varje internationell aktör som ingår i analysen har kapacitetsbedömts. Detta har gjorts utifrån hur stor volym narkotika (hur många kg) de bedöms smuggla in till Sverige per smugglingstillfälle, samt frekvens, det vill säga hur många gånger i månaden de bedöms smuggla narkotika. Detta har sedan upphöjts till årsbasis. Som exempel kan nämnas en aktör som bedöms smuggla 200 kg narkotika, en gång i månaden. Den bedömda kapaciteten på årsbasis blir då 2 400 kilo/år. Materialet som ligger till grund för bedömningarna innehåller information om tidigare, pågående och framtida smuggling av narkotika till Sverige.

Utifrån materialet bedöms de 84 tongivande aktörerna totalt genomföra cirka 850 storskaliga smugglingsförsök per år med vägtransport, där lastbilsflödet är det dominerande smugglingsvägen. Variationen på mängden narkotika per smugglingsförsök är stor mellan aktörerna. Ett 40-tal aktörer bedöms dock smuggla partier som överstiger ett ton per år, vissa upp mot 8 ton årligen. Detta tyder på att narkotikasmugglingen är mycket omfattande. En analys av hur omfattande den totala mängden narkotika som smugglas in i Sverige har gjorts utifrån materialet, där mängden bedöms uppgå till 100-150 ton årligen[15].

Det bör poängteras att det finns flera osäkerhetsfaktorer som skulle kunna innebära att denna bedömning kan vara både en överskattning och en underskattning. Bedömningen grundar sig exempelvis endast på en källa, Encrochat, där informationen som framkommer är svår att validera. Smugglingen i Encrochat omfattar endast hasch, marijuna, kokain och amfetamin. I bedömningen antas vidare att omfattningen och frekvensen är konstant över hela året. Hänsyn har därtill inte tagits till om en aktör har varit frihetsberövad, eller av andra anledningar inte har smugglat under perioden. Sammantaget har det alltså inte varit möjligt att ta hänsyn till olika variationer som kan påverka aktörernas möjligheter till att smuggla narkotika till Sverige inom ramen för bedömningen.

15 De omfattande mängderna återspeglas även i de större beslag som Tullverket har gjort de senaste åren där den genomsnittliga vikten har legat på runt 200 kg per smugglingsförsök.

För att kunna få en mer robust lägesbild av narkotikasmugglingens omfattning behöver denna fråga undersökas mer ingående med källor som kan komplettera uppgifterna från Encrochat.

Det är dock tydligt att de aktörer som har studerats har en mycket hög avsikt och förmåga till frekvent smuggling och avsättning på den svenska narkotikamarknaden. Detta tillsammans med Tullverkets beslagsvolymer vilka på senare år tyder på att de uppskattningar som hittills har gjorts avseende narkotikasmugglingen till Sverige troligtvis är en underskattning. Denna bedömning stärks också av att det de senaste åren och årtiondena har rapporterats om ökad produktion av narkotika, sjunkande priser och ökande renhetsgrader. Även Europol rapporterar om att narkotikautbudet i Europa i dagsläget är avvikande högt.

4.2.1 Bedömning av narkotikamarknadens omfattning

Centralförbundet för alkohol- och narkotikaupplysning (CAN) har tidigare bedömt att konsumtionen av narkotika i Sverige uppgår till ca 15 ton[16]. CAN beskriver att bedömningar av narkotikamarknadens omfattning är osäkra och svåra att göra, då många förhållanden är okända. De beräkningar som redovisas är avsedda att luta åt det försiktiga hållet för att undvika ogrundade överdrifter. Utifrån Encro-materialet går det inte att uppskatta hur mycket narkotika som konsumeras i Sverige, däremot går det utifrån underlaget att bedöma hur mycket som smugglas hit varje år. Denna bedömning, som beskrivs i stycket ovan, leder till ett estimat om att 100-150 ton narkotika smugglas till Sverige varje år. Även om inte all denna narkotika konsumeras i Sverige medför uppgifterna att det finns skäl att förmoda att de bedömningar som tidigare gjorts är i underkant.

[16] Se *Narkotikaprisutvecklingen i Sverige 1988-2019*

5 Penningtvätt

5.1 Inledning

Tillgången till Encrochat har inneburit ett unikt tillfälle att studera omfattningen på de brottsvinster som narkotikahandeln genererar i Sverige, hur de tvättas och omsätts samt vilka roller som är centrala för att hantera brottsvinsterna. Analysen syftar till att höja kunskapen om brottsupplägg och omfattning av illegal penninghantering i Sverige och framhäva de möjliggörare som hanterar aktörernas pengar.

Materialet stärker bilden av att kontanter är det dominerande betalmedlet inom den organiserade brottsligheten då kontanter som motsvarar miljonbelopp hanteras återkommande. Det förekommer även att man använder sig av kryptovalutor vilket möjligen kan bli ett vanligare betalmedel i framtiden.

De uppskattningar av den illegala penninghanteringen som kunnat göras, baserat på bedömningen av mängden narkotika som smugglats in över Sveriges gränser, tyder på att miljardbelopp genereras i narkotikahandeln årligen där stora delar förs ut ur Sverige för återinvestering i nya narkotikapartier. Växlingskontor framstår som centrala i att möjliggöra brottsaktörernas utförsel av kontanter.

Möjliggörarna i materialet rör främst valutaväxlare, insiders på banker och ”låneförmedlare”. Dessa är kritiska för penningtvättsförmågan och bör fortsatt vara strategiska måltavlor i bekämpningen av brottsvinster från narkotikabrottsligheten.

En rad exempel på behov av målvakter och insiders på banker för olika typer av lån, samt konversationer om företag att slussa kontanta medel genom, stärker bilden av att aktörerna är i behov av att få in brottspengar i det legala systemet. Miljardbelopp bedöms även ha omsatts av aktörerna inom varuhandeln i Sverige. Att t.ex. köpa dyra märkesklockor som statussymbol som även kan användas som pant och betalmedel för narkotika framstår som ett utbrett fenomen bland aktörerna. Encrochat användes emellertid främst till narkotikasmuggling varför en tydlig bild inte framkommer av var brottsvinsterna *utanför* själva smugglingskedjan hamnar.

5.2 Tillvägagångssätt för illegal penninghantering

5.2.1 Växling

Valutaväxling framstår i materialet som en eftertraktad och närmast oumbärlig funktion för narkotikasmugglingen. Tillgången till växlare efterfrågas frekvent och det är tydligt att utan möjligheten till valutaväxling hade narkotikahandeln, i dess nuvarande form och omfattning, inte varit möjlig.

Växlingen sker nästan uteslutande från SEK till Euro. Flera av växlarna som framkommer i materialet har drivit en, delvis legal, formell växlingsverksamhet med fysiska kontor vid sidan av den illegala växlingen. Växling kunde också ske med täckmantel av annan företagsverksamhet t.ex. frisörsalong. Ett internationellt kontaktnät är avgörande för att växlingsverksamheten ska fungera och det tycks vara få länder som växlarna inte kan överföra pengar till.

Pengarna förs i första hand ut till Spanien och Nederländerna. Det förekommer att narkotikaorganisatörer som är i behov av växling lämnar pengar till växlaren med hjälp av

via sina medhjälpare (kurirer) i Sverige. Det framkommer även att pengar förvaras i växlarens lokaler eller i andra utrymmen som växlaren tillhandahåller.

Pengarna förs ut ur landet på olika sätt, antingen genom narkotikaorganisatörens försorg eller på annat sätt via involverade växlingsverksamheter, där kurirer troligtvis används för utförseln. Det framkommer i vissa fall att växlaren kontaktar en samarbetspartner i annat land och ber att en utbetalning ska ske till en kurir mot att denne uppger en kod eller annan kvittens som validering för att denne är rätt person och att pengarna lämnats in i Sverige. I övrigt ger materialet ger inte en tydlig bild av hur själva utförseln sker. Lastbilstransport under täckmantel av legal transportverksamhet verkar dock också förekomma.

Att omfattande summor går via valutaväxling kan illustreras inte minst av observationer ur materialet som indikerar att hela 150 miljoner SEK växlades genom endast fem växlare inom loppet av ett par månader. Det bör poängteras att långt fler växlare har identifierats i materialet men att endast dessa fem konton har innehållit tillräckligt med information som har möjliggjort skattningar på konkreta belopp. Det faktum att ett fåtal aktörer summerar en så stor hantering av brottsvinster visar dock på hur central denna verksamhet är för den organiserade brottsligheten. Växlare är den i särklass vanligaste efterfrågade tjänsten i underlaget för penninghantering.

Som uträkning på sid. 25 visar uppskattas miljardbelopp genereras årligen genom försäljning av narkotika i Sverige. De uppskattningar som gjorts tyder vidare på att stora delar av brottspengarna återinvesteras i nya narkotikapartier i utlandet.

5.2.2 Växling kryptovaluta

Vid sidan av överföringar i vanlig valuta finns flertalet exempel på kontanter som växlas till kryptovaluta (främst bitcoins) och förs över till mottagande aktörs e-plånbok. Användningen av kryptovaluta är dock inte särskilt utbredd och frågor om vilken anonymitet det egentligen innebär är återkommande i materialet. Fördelar som framhålls är att det är billigare, eftersom växlaren tar mindre i mellanhand och att det går att skicka pengar utan fördröjning. Det går inte att bedöma användningens omfattning eller utveckling över tid i materialet och den typen av konversation sker sannolikt även via andra kommunikationskanaler än Encrochat. Det är dock tydligt att flera aktörer haft svårigheter att föra ut pengar fysiskt på grund av stängda gränser under Covid-19-pandemin och därför intresserat sig för kryptovaluta. Det är möjligt att pandemin i förlängningen bidrar till att öka kriminella aktörers förmåga att använda kryptovaluta.

5.2.3 Låneupplägg

Efter växling är olika former av låneupplägg det mest frekvent förekommande tillvägagångssättet för illegal penninghantering i materialet. Uppläggen tycks dels handla om rena bedrägerier, dels även som ett sätt för brottsaktörerna att tvätta pengar genom att anskaffa tillgångar som inte hade medgivits med enbart kontanter, såsom bolån. Denna typ av upplägg går troligtvis ut på att lånen betalas av med svarta pengar via målvakter eller betalombud. Behov av blancolån verkar också vara relativt utbrett.

Utöver de aktörer som planerar och genomför låneuppläggen själva förekommer det även att de säljs som en tjänst till andra i materialet. I dessa fall kan tjänsten beskrivas

som "låneförmedling" där låneförmedlaren har ett kontaktnät av målvakter som är villiga att ta lån i sitt namn. Det förekommer att låneförmedlarna har kontakt med banktjänstemän som hjälper till att bevilja lån, acceptera falska löneintyg och höja lånetak.

Låneförmedlarna marknadsför sin tjänst brett och det är inte ovanligt att de tar ut avgift för sin tjänst eller ränta. Tjänsten förutsätter ett kontaktnät med både bankmän och målvakter och är på så vis exklusiv för denna skara. Det framkommer även att banktjänstemän tar betalt för sin tjänst från låneförmedlarna.

I övrigt skickas bilder på kreditupplysningar och kreditbetyg frekvent mellan aktörerna och det talas om bankdosor som ska slås på under telefonkontakt med banktjänsteman, vilket tyder på en omfattande målvaktsproblematik och hantering av målvakters BankID på distans.

5.2.4 Företag i brottslig verksamhet

Företag som används i brottslig verksamhet är det andra finansiella upplägget som framkommer i materialet och det tycks huvudsakligen ske genom 1) att företag startas och används i ett kriminellt syfte, och 2) att företag köps eller övertas för att ”plundras”

I de fall företag används som ett brottsverktyg i penningtvätt handlar det om att få in svarta pengar i ett legalt system. Falska fakturor och bokföringar, samt målvaktsupplägg, är sätt att skikta brottsvinter mellan företagskonton för att dölja pengarnas ursprung. Det kan dels röra sig om att använda befintliga företag som man tar kontroll över, dels att man upprättar företag i syfte att omsätta och tvätta pengar genom.

Låneupplägg genomförs av utnyttjade (kapade) företag som avsiktligt överbelånas för att kunna köpa saker och sedan överges. Låneuppläggen verkar ofta vara beroende av otillbörliga kontakter med banktjänstemän. Liksom privatlånen kan avbetalningen på företagslånen göras med svarta pengar och på så sätt vara ett penningtvättsmodus. I övrigt går det inte att avgöra huruvida syftet är bedrägeri, penningtvätt eller både och.

De aktörer som sysslar med företag tycks ha en relativt hög kunskap om bolagsformer, skattetekniska regler och kontakter till insiders som möjliggör uppläggen.

5.2.5 Parallell marknad

Utifrån de uträkningar som har gjorts på narkotikaförsäljning och utförsel av brottspengar, skattas 700 miljoner kronor i brottsvinster ha kvarstannat i Sverige under perioden som studerats[17]. Långt ifrån alla aktörer talar i sina chattar om finansiella upplägg och penningtvätt av brottsvinster. Detta kan bero på att Encro i första hand är ett verktyg för narkotikasmuggling, men det ger också anledning att anta att det finns en parallell marknad där de kontanta brottsvinsterna också kan omsättas relativt obehindrat.

Blocket framkommer som en frekvent handelsplats för aktörerna när det gäller klockor och bilar. Vidare förekommer enstaka exempel på hyreskontrakt som köps för kontanter, och det finns rimligtvis fler exempel på liknande fenomen som *inte* uttalas.

Klockor som statusmarkör och betalmedel för narkotika, pant eller handelsvara omnämns genomgående i materialet. En grov uppskattning baserat på tillgängligt bild-

17 Upphöjt till årsbasis utgör brottsvinsterna 2,8 miljarder sek som redovisats i avsnitt 5.4 ”Omfattning av illegal penninghantering”

material är att klockor till ett värde om ca 16 miljoner kronor cirkulerat bland aktörerna. Klockor är den i särklass vanligaste ”dyra” tillgången som framkommer i materialet.

Vidare cirkulerade fotografier på kontanter till ett värde av *minst* 50 miljoner kronor bland aktörera under aktuell period (ej årsuppskattning). Kontexten för dessa kontanter framkom inte alltid men de var troligtvis föremål för växling eller tillfällig förvaring.

5.3 Centrala möjliggörare

5.3.1 Växlare

De växlare som studerats i materialet är ofta män i 50-årsåldern med lång erfarenhet av valutaväxling och överföring. De har sällan någon direkt tillhörighet till ett kriminellt nätverk eller är verksamma i någon annan del av aktörernas brottslighet.

Deras kontaktnät är dock stort och spänner över kriminella aktörer i flera regioner. Det finns även vissa exempel på personer i växlarnas närhet som tycks förmedla kontakt mellan behov av växling och själva växlarna. Detta görs mot en procentuell ersättning av växlingsbeloppet. Dessa personers förmedling kan fylla funktionen av ett säkerhetsfilter för att växlarna ska kunna lita på de kriminella kunder som hör av sig. Leverans, upphämtning och utförsel av växlade summor utförs dock i huvudsak av medhjälpare/kurirer till de kriminella aktörerna.

Vad gäller "kryptoväxlare"[18] är materialet mycket begränsat. Det är dock *inte* troligt att samma typ av "möjliggörar-roll" skulle uppstå om användningen av kryptovaluta ökade, detta då det finns andra tekniska lösningar för sådan växling.

5.3.2 Låneförmedlare

De aktörer som erbjuder låneupplägg som en tjänst för penningtvätt eller bedrägeri är allt som oftast involverade i den övriga narkotikabrottsligheten i materialet. De kan dock inte kategoriseras som de mest tongivande narkotikaorganisatörerna.

Låneförmedlarna är oftast i 20- till 30-årsåldern med ett mer begränsat kontaktnät än växlarna. Låneförmedlarna har en viss kompetens, kunskap och kontaktnät inom banksystemet.

De aktörer som använder låneupplägen som ett sätt att tvätta pengar å andra sidan är troligtvis de som gör så pass stora vinster på sin narkotikabrottslighet att endast en kontant ”parallell” marknad inte är tillräcklig för att konsumera upp vinsterna.

5.3.3 Insiders: banktjänstemän, revisorer, mäklare

Banktjänstemän är en vanligt förekommande insider i materialet. Dessa framstår ofta som en förutsättning för att kunna genomföra låneupplägg och använda företag i brottslig verksamhet.

Det finns också exempel på mäklare och revisorer som möjliggör upplägen genom att godkänna falska bokföringar och dokument. Mäklare förekommer också i termer av att ge kriminella aktörer förtur till hyresrätter i nybyggda flerfamiljshus.

18 Person som handlar med kryptovaluta.

5.3.4 Varuhandlare

Givet den bredd på märkesklockor som framkommer i materialet är det troligt att åtminstone en del av brottsaktörerna i något skede inhandlat dessa hos registrerade klockhandlare som därmed möjliggör aktörernas penningtvätt. Klock- och bilhandlare förekommer dock sällan eller aldrig i materialet varför en beskrivning av dem inte låter sig göras i denna analys.

Blocket är den marknadsplats som förekommer mest tydligt i materialet. Blocket utgör troligen en stor och svårkontrollerad plattform där aktörerna kan tvätta sina pengar. Det finns exempel på behov att köpa varor på Blocket kontant där avsikten är att snabbt sälja och därmed få in kontanterna på bankkonto.

5.4 Omfattning av illegal penninghantering

De internationella organisatörernas penningflöden är intressanta att uppskatta för att få en fingervisning om omfattningen av penningflödena som följer av försäljning i följande led på den svenska interna marknaden. I beräkningen av omfattningen nedan finns inte uppgifter om varken distributörsledens eller gatuförsäljningsledens brottsvinster. Detta avsnitt fokuserar på de internationella organisatörernas vinster. Det innebär att den *totala* vinstumman av *samtliga* led som narkotikapartierna passerar innan de når gatunivån överstiger de summor som beräknas i denna rapport. I figur 2 illustreras fyra steg i handeln som kan kopplas till de internationella narkotikaorganisatörernas införsel.

Figur 2. Penningflöden baserat på de internationella organisatörernas årliga införsel av narkotika till Sverige i SEK. Kretsloppet utgår från ett inflöde av narkotika till Sverige om 150 ton årligen. I löptexten nedan anges ett vidare spann om mellan 100-150 ton årligen.

1) Det stora kretsloppet i bilden, ”brottsinvestering”, illustrerar de internationella aktörernas investering, försäljning och återinvestering i narkotikapartier. De internationella organisatörerna köper partier till grossistpris antingen direkt av producenterna, eller indirekt via kriminella nätverk som agerar grossister åt producenterna. Som nämns i narkotikaanalysen uppskattas upp mot 100-150 ton föras in i Sverige på årsbasis. Justerat per preparat motsvarar det en investeringskostnad på 8,3 miljarder SEK vid 100 ton, och vid 150 ton 12,5 miljarder SEK.
2) Narkotikan förs in i Sverige och säljs till de nationella organisatörerna[19] (”första ledets distributörer”). Värdet för 100 respektive 150 ton narkotika, justerat per preparat, motsvarar ett försäljningspris på mellan 10 och 15 miljarder SEK.
3) Merparten av värdet från försäljningen återinvesteras av de internationella organisatörerna i nya narkotikapartier. För att på ett teoretiskt plan beräkna hur stor andel av försäljningen som återinvesteras görs antagandet att återinvestering sker av samma mängd narkotika som uppskattats föras in årligen, alltså 100-150 ton. Ett försäljningsvärde på 10-15 miljarder kronor och en återinvestering, som antas vara konstant på 8,3–12,5 miljarder (för 100-150 ton), medför att 80 procent återinvesteras.
4) Resterande 20 procent, alltså vinstmarginalen mellan försäljning och återinvestering, utgör 1,8- 2,8 miljarder kr, i bilden betecknat som det mindre kretsloppet ”brottsvinster”. Det är dock viktigt att poängtera att omkostnader som transport, logistik, förvaring och beslagtagna narkotikapartier inte har inberäknats, varför vinsten och omsättningen är lägre än vad som beräknats här.

19 En aktör som har förmåga att organisera distribution av narkotika inom Sverige.

6 Vapen och sprängmedel

6.1 Inledning

Som nämnts i avsnitt tre (våld) bedöms vapentillgången inom den organiserade brottsligheten som god, då vapen finns tillgängligt bara ett eller två steg bort från när aktörer efterfrågar dem. Till skillnad från narkotikasmugglingen, som beskrivs i avsnitt 4, visar det analyserade materialet inte på något som tyder på någon större organisering eller systematik vad gäller vapeninförsel. Materialet från Encrochat är främst orienterat runt narkotikabrottslighet. Det är i förhållande till materialet i övrigt endast en liten del av aktörerna som under tidsperioden har vapen och sprängmedel som primär aktivitet (det vill säga, inte som bisyssla vid sidan av narkotikahandel). Följande analys är baserat på dessa konton.

6.2 Införsel tillgång och förvaring

6.2.1 Vapen

Materialet tyder på att införsel av vapen sker genom att mindre partier smugglas in av enskilda kurirer eller tillsammans med narkotikapartier. Det är stor variation på de olika typer av vapen som smugglas in, detta talar för att vapenmarknaden troligen är decentraliserad, och att det inte finns några stora lager.

Aktörerna har vapenkontakter i Balkanländerna samt i Polen, det vill säga länder som Sverige historiskt haft illegal vapeninförsel ifrån. Mest troligt är att de illegala vapnen kommer in till Sverige via fordons- och färjetrafiken.

Olika slags vapen tas in från olika länder. Aktörerna tar det som de kommer över och smugglar på det sätt som passar för stunden, ofta i mindre försändelser vilket också kan vara en förklaring till varför nätverken har en spridning av vapentyper i sina ”arsenaler”. En metod för smuggling av narkotika som uppmärksammats i materialet är att legala fraktbolag används. Det finns konton i materialet som bekräftar att fraktbolag även används i syfte att smuggla vapen. Aktörerna betalar sin kontakt, t.ex. en chaufför, mellan 250-500 EUR mot att denne ser till att aktuellt paket levereras till önskad destination. Kontakterna på budfirmorna beskrivs som goda och verkar ha utnyttjats under flera år.

Av materialet framgår vidare att inköp av vapen sker på individnivå, det vill säga inte som ett gemensamt köp av ett nätverk. Ofta går det att härleda efterfrågan av vapen till att en personlig konflikt nyligen uppstått.

Förvaring av vapen sker oftast ett par steg bort från ägaren eller brukarna. Vapnen förvaras i lägenheter, fordon eller hos individer utan uppenbar koppling till ägaren eller brukarna, eller utomhus. Det förekommer att ett antal individer har gemensamma nycklar till förvaringsplatsen, för att kunna låna, ge bort, använda eller flytta vapnet. Främst väljs platser som inte kan kopplas till någon specifik person inom nätverket eller gruppen. Det kan vara bekanta och flickvänner man litar på och har förtroende för, men till vilka polisen inte skulle ha en naturlig ingång vid en kontroll av den kriminelle individen, troligtvis har dessa personer ”rena” brottsregister. Flera vapen förvaras sällan på en och samma plats utan sprids i regel ut över flera platser. De personer i gruppen som

behöver ha tillgång till vapnen har också nycklar till någon eller några av platserna. Nycklar byts med varandra beroende på vilka som behöver tillgång för stunden.

Vapen som använts vid brott kan komma att återanvändas, det finns exempel då vapenägare lånat ut sitt vapen och återfått det väl rengjort efter utfört våldsdåd. Det framstår som vanligare att de vapen som återanvänds är av kändare märken så som Glock och Walther. Detta bedöms bero på att de har högre renommé och blir en form av statussymbol.

6.2.2 Ammunition och sprängmedel

Tillgång och handel avseende ammunition är vidare ingen begränsande faktor för aktörerna. Detta kan troligen förklaras med att vapenmagasin inte är licenspliktiga, att handel med ammunition inte är reglerad på samma sätt som handel med vapen samt att ammunition är lättare att smuggla än vapen. Det är lättare att köpa ammunition till 9mm pistoler men det är svårare att köpa ammunition till automatvapen som till exempel Kalashnikov och Zastava M70 som är bland det mest vanligast förekommande automatvapnet bland kriminella.

När det gäller tillgång och handel med sprängmedel, så tycks fler personer bli inblandade än vad som är fallet vid vapenhandel. Sprängmedlet anskaffas troligtvis inom Sverige, men materialet ger ingen indikation om specifika orter eller företag. Det finns heller inget i materialet som pekar på att sprängmedel eller komponenter smugglas in till Sverige. Anskaffandet av sprängmedel ser lite annorlunda ut för olika grupperingar.

Under den särskilda händelsen Rimfrost uppmärksammade Polismyndigheten att flera kriminella individer antingen själva innehade företag med sprängverksamhet eller hade någon i nära anslutning som hade det. Materialet stödjer den tidigare teorin om att det illegala sprängmedlet med dess komponenter kommer från den legala marknaden i Sverige.

Behovet av krypterade kommunikationstjänster är tydligt även för vapenhandeln: I konversationerna diskuteras vapen och handel med dessa helt öppet, men vapendiskussionerna avslutas inte utan detta sker troligen via röstsamtal, samt via andra system.

7 MC-relaterad kriminalitet

7.1 MC-miljön och samverkan

Analysen visar att de kriminella MC-gängen fortfarande är en maktfaktor. MC-gängen är självförsörjande och har ständigt tillgång till narkotika, vapen och sprängämnen. Gängen har kvar sina platser på den kriminella scenen och underhåller löpande sitt våldskapital genom olika typer av våldsbrott.

Aktörerna med koppling till MC-miljön har nästan dubbelt så stora kontaktnät jämfört med genomsnittet av användarna på Encrochat. De har också ett högre antal utlandskontakter, högre trafikvolym och kopplas mot fler brottsområden än övriga brukare. I materialet framgår att medlemmarna löpande samverkar med andra nätverk och aktörer.

7.2 Brottsupplägg

I materialet har ett antal personer identifierats, som befinner sig runt aktörerna och bedöms ha viktiga funktioner för aktörernas kriminella upplägg. Dessa personer är själva inte medlemmar i någon MC-klubb

Majoriteten av MC-aktörerna har genom ett antal personliga kontakter byggt upp egna organisationer med utförare och ”springpojkar”. Dessa används för att utföra uppgifter som narkotikatransporter, lagerhållning och indrivning och är överlag i inte identifierade som MC-medlemmar, kopplingen verkar snarare vara av personlig karaktär. Det framgår tydligt att aktörerna och deras springpojkar inte ska observeras tillsammans på offentliga platser. Det ska inte heller gå att koppla aktörerna till specifika adresser eller fordon vid ett eventuellt polisingripande. Flera aktörer har även kopplat ett antal ”gröna personer” till sin organisation. Med gröna personer avses vanligtvis laglydiga medborgare utan koppling till vare sig medlemmen eller till polisiära system. De gröna personerna, vilket ofta är kvinnor, har sällan kännedom om helheten utan avlönas enkom efter uppdrag.

Kommunikationskedjorna som framträder i materialet, och som går att följa tack vare tillgång till det krypterade materialet, visar att den utförare som slutligen åtar sig uppdraget, ofta befinner sig flera led ifrån den anstiftande aktören. Kedjan ser ofta ut som följande: Aktören lägger ut ett uppdrag på en ”springpojke” som i sin tur, via ett annat krypterat kommunikationssystem, kontaktar en utförare (exempelvis en transportör). Utföraren, eller transportören som i det här exemplet, genomför uppdraget alternativt kontaktar utföraren en ”grön person” som utför uppdraget.

8 Otillåten påverkan

Kriminella aktörer utövar otillåten påverkan i syfte att skydda eller främja brottslig verksamhet. Otillåten påverkan inbegriper trakasserier, hot, våld, skadegörelse, otillbörligt erbjudande (korruption) och otillbörlig relation (nepotism). Otillåten påverkan riktas mot personer med anledning av deras yrkesutövning eller deras roll i rättsliga processer. I den förstnämnda kategorin ingår t.ex. politiker, offentliganställda tjänstemän, företrädare för media samt personer vars underlag har betydelse för myndighetsutövning (såsom läkare) och anställda inom det privata näringslivet (såsom banktjänstemän).

I syfte att få en bild av vilka yrkeskategorier som de kriminella aktörerna i Encrochat utövar otillåten påverkan mot användes följande sex underkategorier (utfall i parantes efter respektive kategori): Politiker i riksdagen och i kommunfullmäktige (1), Tjänsteman inom statlig och kommunal förvaltning (5), Tjänsteman inom rättsväsendet inkl. polis (2) Advokat (30-31), banktjänsteman (5). Totalt rör det sig om 43-44 fall av otillåten påverkan, där den övervägande delen riktas mot advokater.

Samtliga fall av otillåten påverkan handlar om otillbörligt erbjudande. I de flesta konversationer berörs inte kompensationen för de tjänster som efterfrågas. Ett grundläggande antagande bör dock vara att en person inte utför en tjänst som innebär ett visst risktagande utan att vilja ha ersättning.

I materialet förekommer en konversation där en aktör avser att muta en politiker på kommunal nivå. Politikerns namn framkommer inte.

Det förekommer även uppgifter om att de kriminella aktörerna har kontakt med tjänstemän på olika myndigheter. Enligt konversationerna förser dessa kontakter de kriminella aktörerna med information eller utnyttjas på andra sätt inom ramen för sin tjänsteutövning.

Inom banksfären har fem kriminella aktörer kontakter som bistår dem att begå brott. En av de kriminella aktörerna har kontakt med en banktjänsteman som beviljar de personer som aktören anvisar honom, bolån åtta gånger årsinkomsten istället för de gängse fyra. Materialet ger vid handen att brottsligheten är omfattande och involverar flertalet personer. En aktör har kontakt med en banktjänsteman som bistår vid bedrägerier. Denne har ett kontaktnät bestående av banktjänstemän och revisorer som mot betalning utför tjänster. En annan aktör som har flera bankkontakter som beviljar banklån. En av kontakterna tar 450 000 kronor i ersättning för ett lån på tre miljoner kronor.

9 Slutord

Att Polismyndigheten har kunnat ta del av material från Encrochat har inneburit en ökad inblick i de kriminella aktörernas motiv, tillvägagångssätt och strukturering. En tydlig insikt utifrån analysen av materialet är att flera av de kriminella aktörerna i det närmaste verkar sakna spärrar för att utsätta sina antagonister för dödligt våld när de anser att det är motiverat. Det finns inte några påtagliga praktiska hinder för att utföra grovt våld – anstiftarna bakom våldet har i regel vare sig svårt att ordna med vapen och ammunition, medhjälpare eller att hitta en person som kan utföra våldet. Våldet i sig kan vara motiverat av narkotikauppgörelser men drivs också av personliga konflikter, hämndspiraler eller utförs för att undvika att själv bli angripen. Vidare tydliggör materialet att den mängd narkotika som smugglas till Sverige är mycket omfattande. Den ekonomiska drivkraften bakom narkotikahandeln är påtaglig och den omsätter stora belopp.

När det gäller organiseringen i kriminella nätverk framstår det som att majoriteten av Encro-användarna inte begränsar sina samarbeten till personer inom det egna nätverket. Snarare tycks många samarbeten vara projektbaserade och tillfällesstyrda där de kontakter som behövs för att lösa en uppgift tas. Aktörerna beskriver även att de har korrupta kontakter inom bankväsendet samt på myndigheter och företag.

Aktörerna har överlag goda möjligheter att knyta de kontakter som krävs för att de ostört och framgångsrikt ska kunna fortsätta bedriva sin brottslighet. I detta avseende är tillgången till en krypterad kommunikationskanal en avgörande förutsättning som både möjliggör organisering av storskalig narkotikasmuggling och underlättar koordineringen av våldsbrott. Även om insatsen mot Encrochat kan ha haft en avskräckande effekt fortgår kommunikationen på andra liknande krypterade plattformar.

Under arbetet med Encrochat har tre betydande sårbarheter i samhället blottlagts. Dessa sårbarheter riskerar att medföra en eskalerad negativ utveckling om de inte åtgärdas. Sårbarheterna utgörs av följande:

- *Att rättsväsendet inte är dimensionerat för storleken på narkotikamarknaden* – materialet indikerar att narkotikasmugglingen till Sverige, och därmed även hanteringen och konsumtionen, är betydligt mer omfattande än vad de samhällsinstitutioner som har till uppgift att hantera denna problembild är dimensionerade för. Detta gäller såväl rättsväsende som t.ex. sjukvård och sociala verksamheter.

- *Att unga personer ofta rekryteras för att utföra grovt våld* – det är påfallande lätt för en anstiftare att rekrytera en ung person för att utföra till exempel en skjutning. Att det finns ett stort antal unga personer som är beredda att utföra dödligt våld på beställning är symptom på en problembild som spänner över samhället i stort.

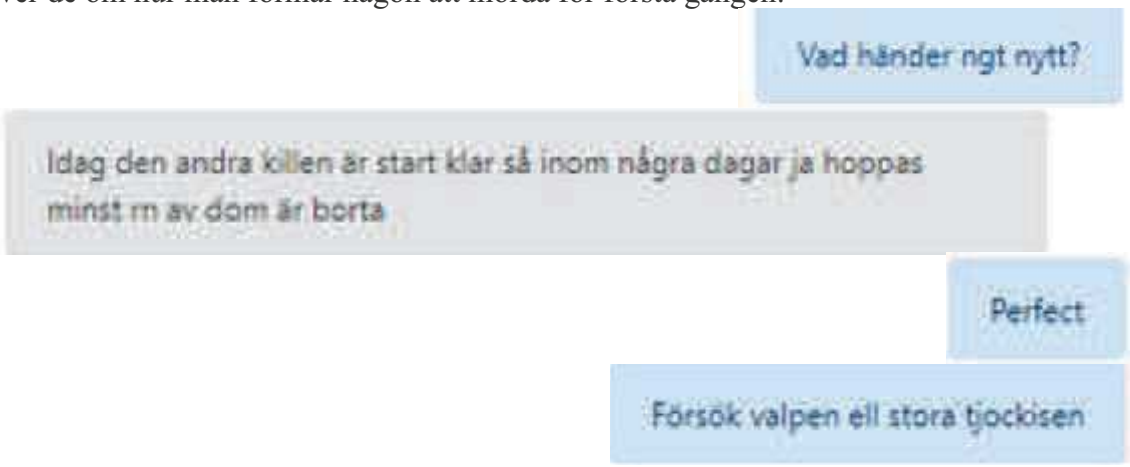
- *Att myndigheter och företag är sårbara för insiders, otillåten påverkan och korruption* – kriminella aktörer inom den organiserade brottsligheten har ett intresse av att utnyttja personer inom samhällsviktiga yrkesgrupper i brottsupplägg. De kriminella kan med olika metoder försöka säkerställa att de har tillgång till myndighets- eller företagsanställda för att tillgodose detta intresse.

Möjligheten för de brottsbekämpande myndigheterna att bedriva ett framgångsrikt arbete mot den organiserade brottsligheten har en avgörande betydelse för att minimiera de sårbarheter som beskrivs ovan. För att ha möjlighet att förbygga, upptäcka och förhindra grov organiserad brottslighet är underrättelsetjänstens tillgång till krypterad kommunikation mellan aktörerna av stor betydelse.

Bilaga 1. Utdrag från konversationer i Encrochat

En uppdragsgivare stämmer av att den person som han har anlitat för mord fått pistolen som han ordnat:

Samma person skriver senare med en vän om hur det går med mordplanerna. Bl.a. skriver de om hur man förmår någon att mörda för första gången:




Just nu ja har inte råd o va kräsen den av dom han tar ja är nöjd men har sakt bästa är om du tar 2 på en o samma gång
Ja d å jakpot om d å 2
Hur säker å du på denna kille
Har han kört innan?
Bror han har tjatat på att få göra jobbet ett tag så han är själv sugen på det
Har han tryckt av?
Nej
Offffff den å jobbig
O han ska göra d sj?
Men någon gång måste va första gången för alla
Bror fins några manusjor som har det här i säg
O den här killen är snud på cyckos
Ja tror han får jobbet gjort
Ja bror men nör vo va yngre vi tog alltid i gbg med oss folk en ggn o dom fick va med o se ell va med trycka eftee vibtryckt
D å jäääte svprrt ongöra sj flrsta ggn såndu vet
Men du måste prata rät

En person får i en konversation hjälp av en kontakt att skaffa vapen:

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
1.1 Bakgrund 1
1.2 Syfte 1
1.3 Avgränsning 1

2 INTRODUKTION 2
2.1 Kort beskrivning av Android 2
2.2 Telefonfabrikat 2
2.3 Inköp 2
2.4 Operatör 3
2.5 Identifikation 3
2.6 Android OS 3
2.6.1 Lösenordsskydd 3
2.6.2 Applikationer 4
2.7 Encrochat OS 4
2.7.1 Lösenordsnivåer 4
2.7.2 Språk 4
2.7.3 Tid och tidszon 5
2.7.4 Positionsdata 5
2.7.5 Applikationer 5

3 KÄLLOR 9

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.

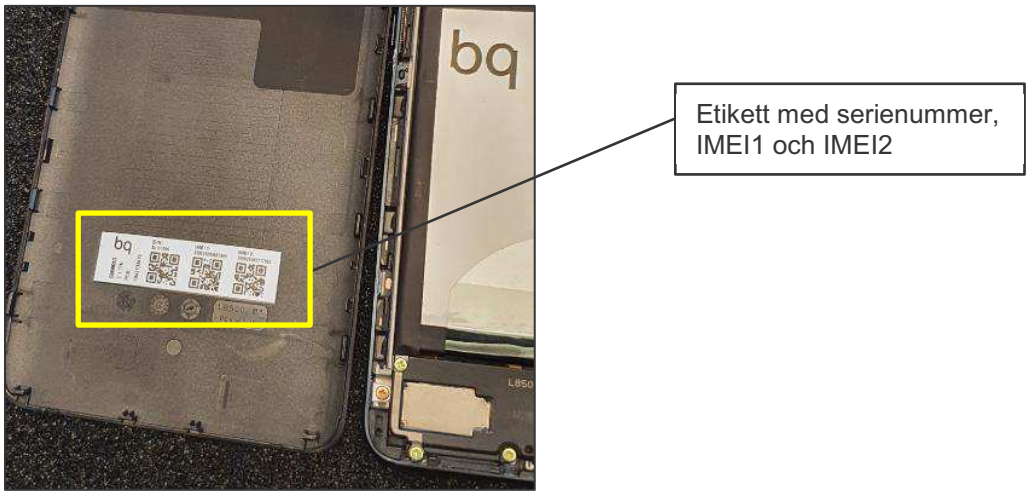


Bild 1 – Insidan av bakstycke på BQ Aquaris X2

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.

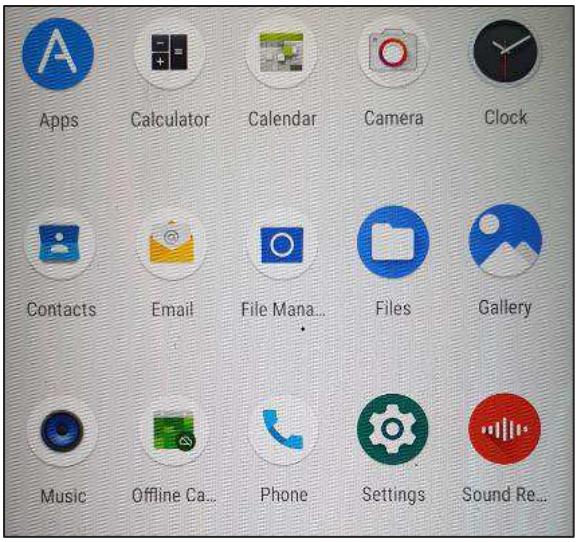


Bild 2 – Applikationer i Android OS på BQ Suro Carbon

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.

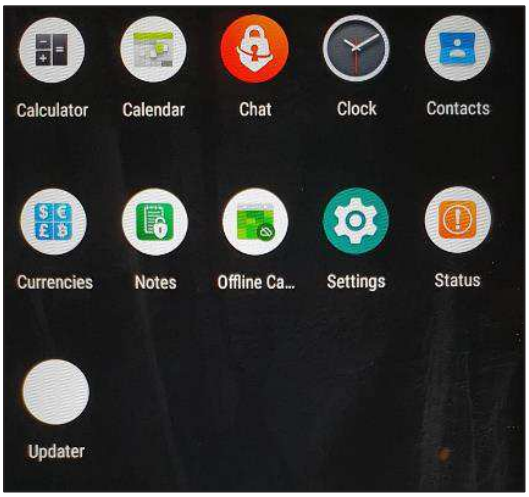


Bild 4 - Applikationer i Encrochat OS på BQ Suro Carbon

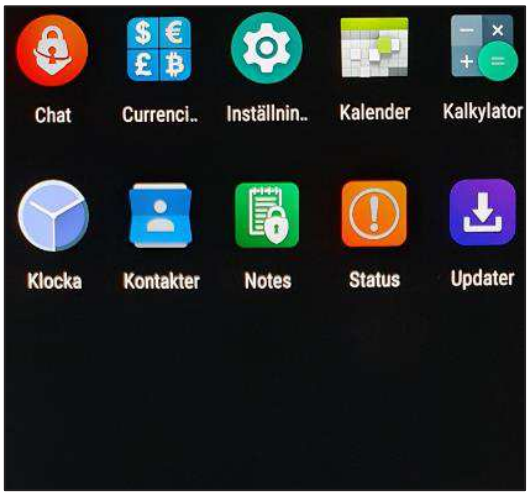


Bild 5 - Applikationer i Encrochat OS på BQ Aquaris X2

[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.

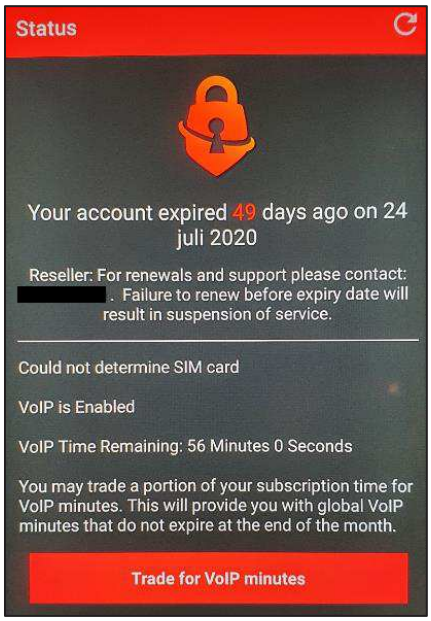


Bild 6 - Applikationen Status (maskerat reseller-användarnamn)

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.

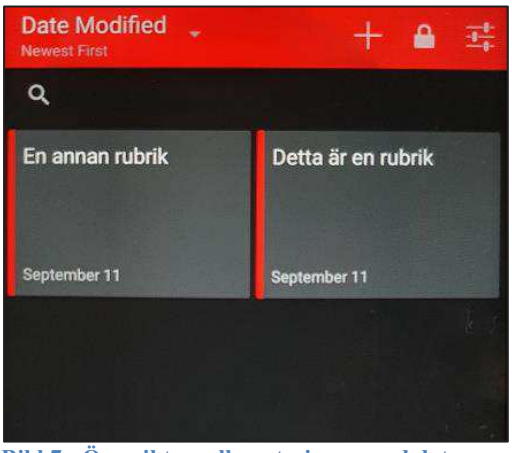


Bild 7 - Översikt av alla noteringar med datum

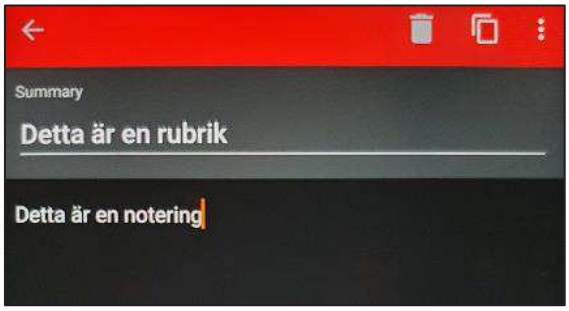


Bild 8 - En notering

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.

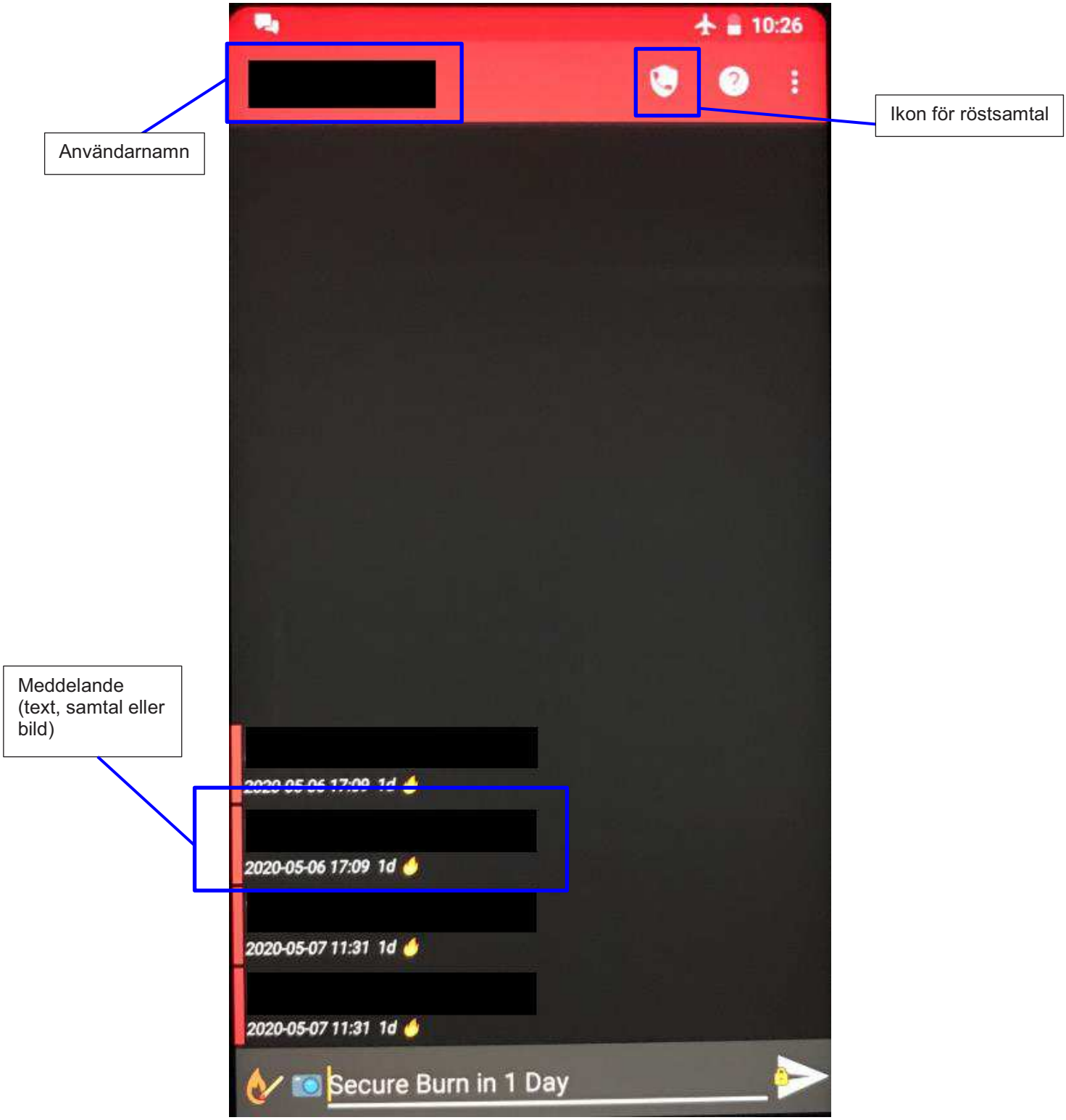


Bild 9 - Vy över en kontakt i applikationen Encrochat

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

Datum
2021-05-20

Polismyndigheten
Nationellt Forensiskt Centrum
Linköping

Förtydligande

I NFC IT Notat 2020-09 Förkonfigurerade enheter finns följande stycke:

> ***2.7.4 Positionsdata***
> *På de telefoner som har observerats har inställningen platstjänster 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 för användaren i enheterna och är inget NFC har möjlighet att uttala sig om.*

NFC kan inte uttala sig om vilken basstation som enheten har kontakt med eller vilken information som sedan har inhämtats av annan part. Nedanstående formulering beskriver det kunskapsläge som NFC besitter.

> ***2.7.4 Positionsdata***
> *På de telefoner som har observerats har inställningen platstjänster inaktiverats eller helt plockats bort vilket har till följd att enheterna inte kan platsbestämmas. Det avtryck som enheterna lämnar uppstår i kontakten med mobilnätet och dess basstationer. Denna information och dess precision är inte synbar för användaren i enheterna och är inget NFC har möjlighet att uttala sig om.*

2021-05-20 Informationstekniksektionen
Nationellt Forensiskt Centrum

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.

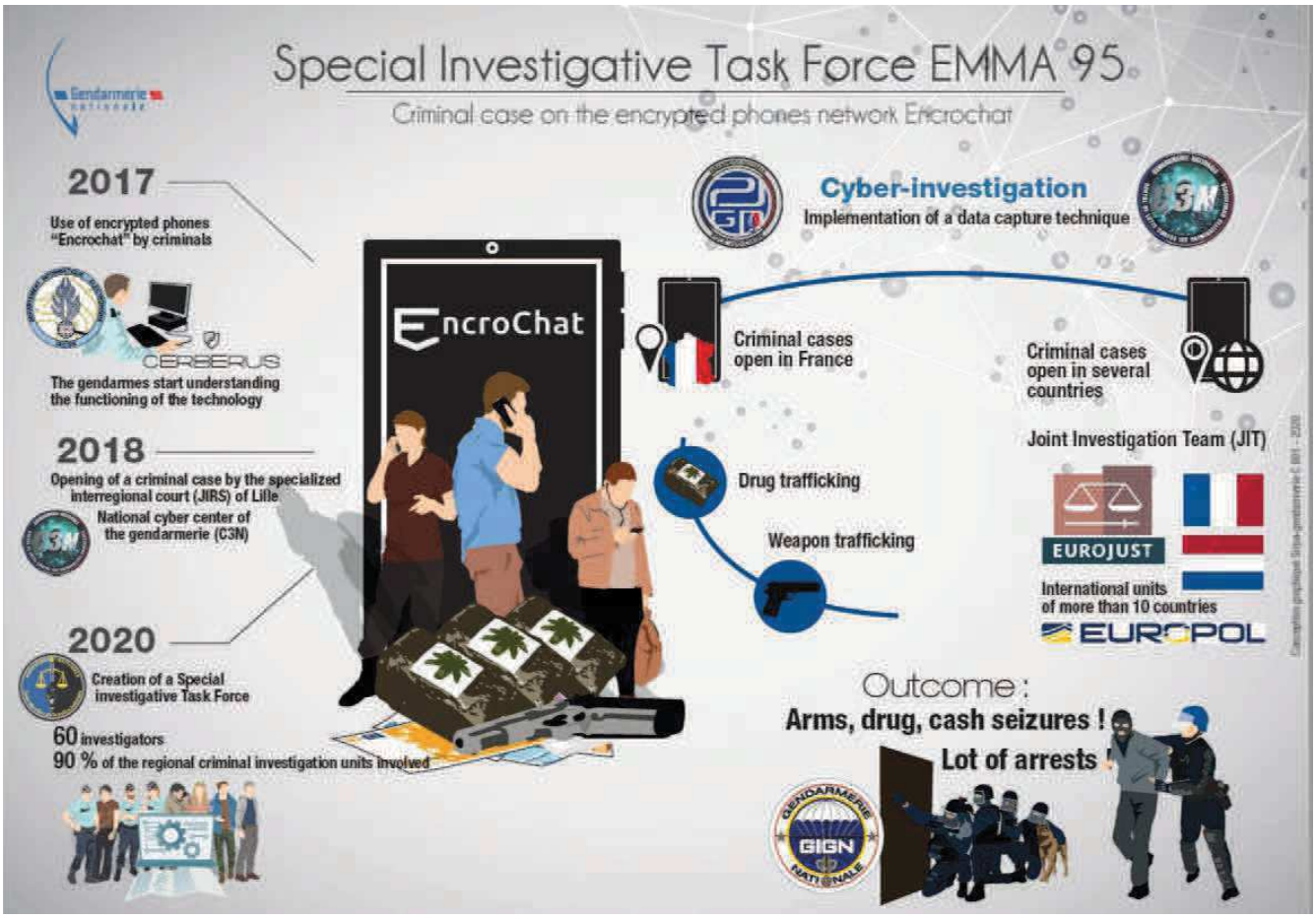
Interregionala specialdomstolen vid regiondomstolen i Lille har inlett en förundersökning gällande den krypterade kommunikationslösningen EncroChat med anledning av lokalisering av de servrar som säkrar processen.

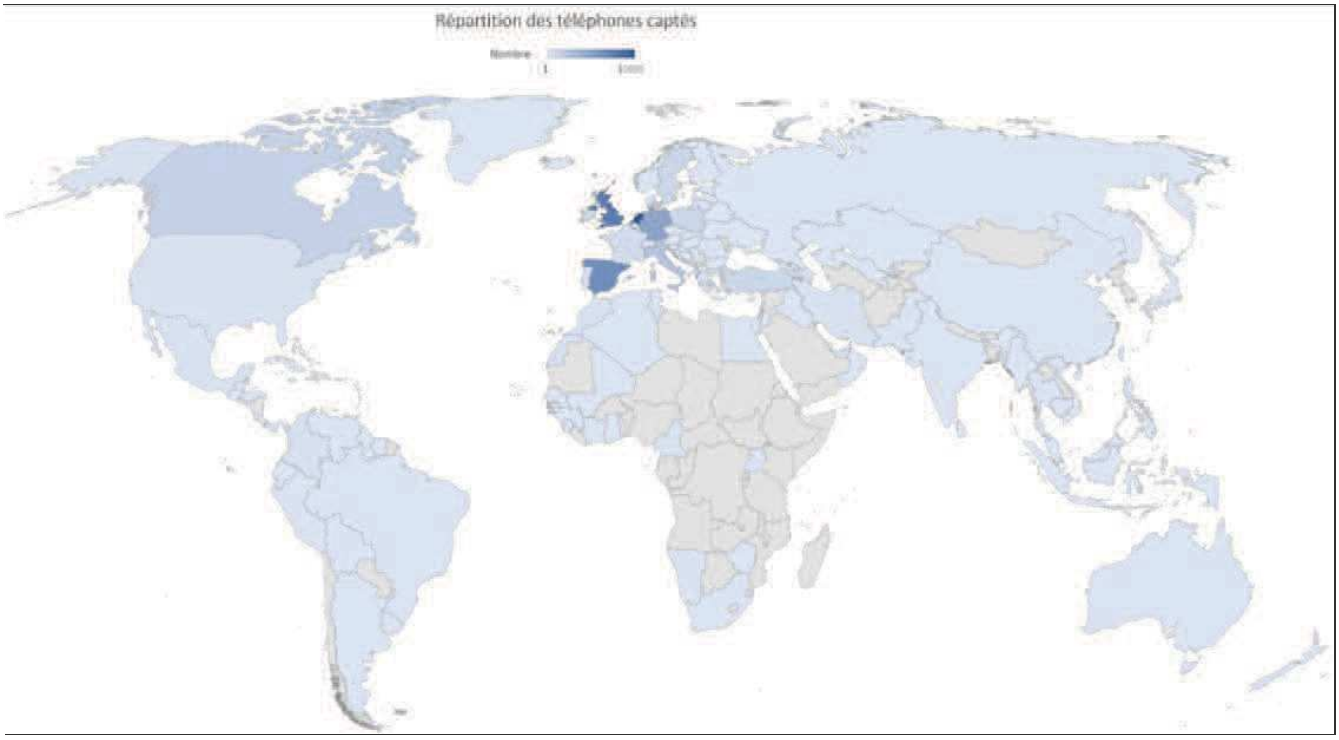
- **<u>Den gemensamma utredningsgruppen</u>**

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
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 !
GIGN


Répartition des téléphones captés

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.

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

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
1.1 Bakgrund 1
1.2 Syfte 1
1.3 Avgränsning 1

2 ANALYS 2
2.1 Begrepp 2
2.2 Blackberry 3
2.2.1 Blackberry-applikationer 3
2.3 Karaktär av ärenden 4
2.4 Operatör 4
2.5 Pris 4
2.6 Sky Global 4
2.7 Applikationen SkyECC 5
2.7.1 Inloggning 5
2.7.2 Identifiering 6
2.7.3 Valv 6
2.7.4 Chatt 7
2.7.5 Broadcast 7
2.7.6 Grupper 8

3 SLUTSATS 8

4 KÄLLOR 9

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).

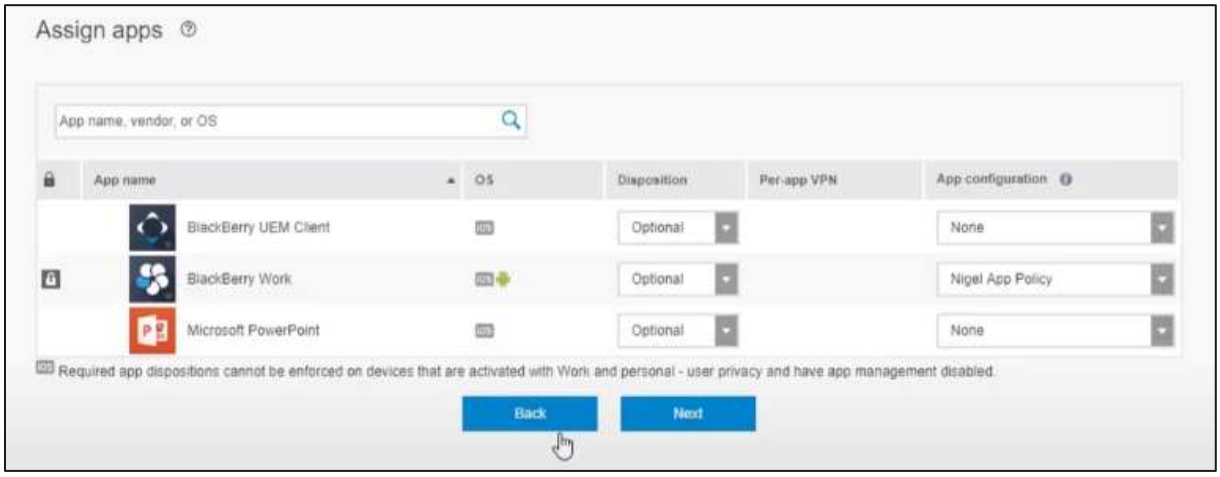


Bild 1 - Vy för att tilldela applikationer (Källa: Blackberrys användarmanual).

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.

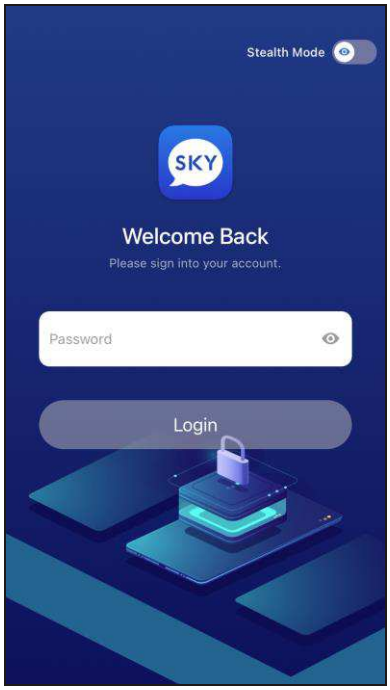


Bild 3 - Inloggningsrutan för SkyECC

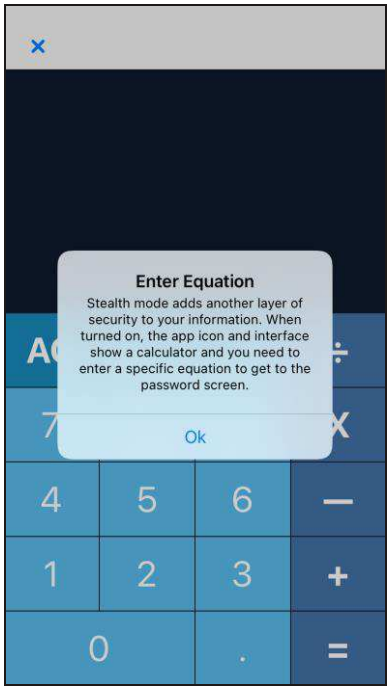


Bild 4 - SkyECC i Stealth mode

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.

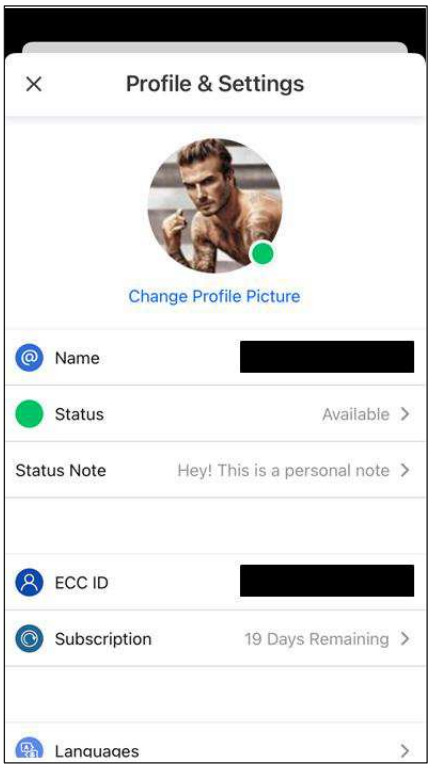


Bild 5 - Användaruppgifter

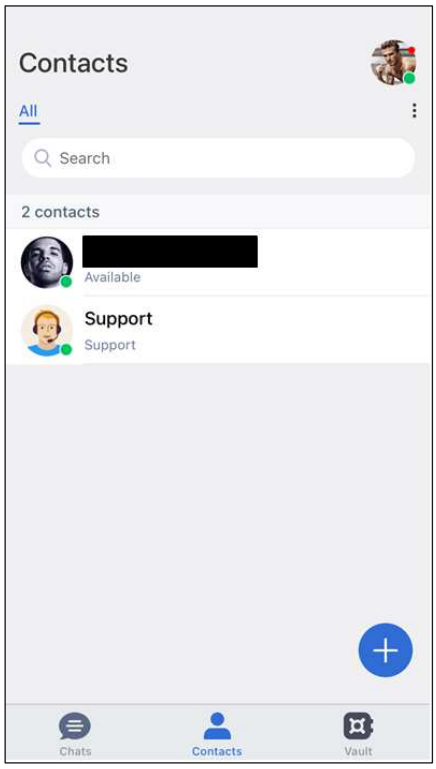


Bild 6 - Kontakter

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.

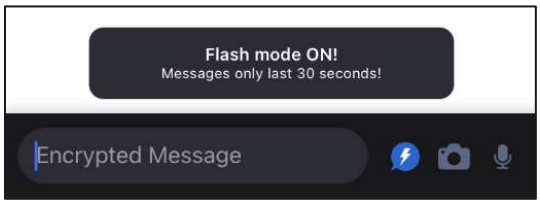
Chattmeddelanden
Vanligen raderas chattmeddelanden efter en förutbestämd tid, dock går det att spara meddelanden i valvet.

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
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’.

Polisen

Bilaga - Skäligen misstänkt

Enhet	Diarienr
Region Nord, Aktionsgrupp 1 Rgn Nord	5000-K601538-21

Skäligen misstänkt person	Identifierad	Anledning	Personnr
Lanuza, Björn Luis	Nej		19850915-7478

Polisen

Personalia och dagsbotsuppgift

Utskriftsdatum
2022-05-24

Namn			Personnummer
Lanuza, Björn Luis			19850915-7478
Tilltalsnamn	Kallas för	Öknamn	Kön
Björn			Man
Födelseförsamling	Födelselän	Födelseort utland	
Sofielund			
Medborgarskap	Hemvistland	Telefonnr	
Sverige		0721903165: Arbetstelefon	
Adress		0700470082: Mobiltelefon	
Paseo Jesus Santos Rein Apt 1010 29640 Fuengirola Spanien			
Folkbokföringsort		Senast kontrollerad mot folkbokföring	
		2020-12-08	

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	0	3
Försörjningsplikt		Skulder
Nej, inte utöver barn.		100000
Förmögenhet		
0		

Kontroll utförd

Taxerad inkomst	Taxeringsår
0	2019
Taxeringskontroll utförd av	Datum
Pinsp J Englund	2020-05-26

Polisen

Underrättelse/Delgivning jml RB 23:18a

Enhet
Region Nord, Aktionsgrupp 1 Rgn Nord

Ärende

Diarienr
5000-K601538-21

Handläggare
Lind, Robin

Gärning
Grovt narkotikabrott

Berörd person

Personnr	Efternamn	Förnamn
19850915-7478	Lanuza	Björn Luis

Underrättelse utsänd	Yttrande senast	Underrättelse slutförd	Delgiven info. om ev. förenklad delgivning
2022-03-30		2022-05-24	

Underrättelsesätt
Mail till häktet Kronoberg

Notering
Utredningsmaterialet översänt via mail till häktet Kronoberg och den misstänkte.

Datum
2022-05-02

Erinran
2022-05-02: Önskar ytterligare två veckor för att gå igenom utredningsmaterialet, vilket beviljas av åklagare.

2022-05-24: Försvarare och misstänkt uppger att det går bra att redovisa ärendet idag.

Försvarare

Namn
Andersson, Elsa

Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
2022-03-31		2022-05-24

Underrättelsesätt
Via post

Notering
Utredningsmaterial på CD-skiva översänt via post till advokat.

Datum
2022-05-02

Erinran
2022-05-02: Önskar ytterligare två veckor för att gå igenom utredningsmaterialet, vilket beviljas av åklagare.

2022-05-24: Försvarare och misstänkt uppger att det går bra att redovisa ärendet idag.