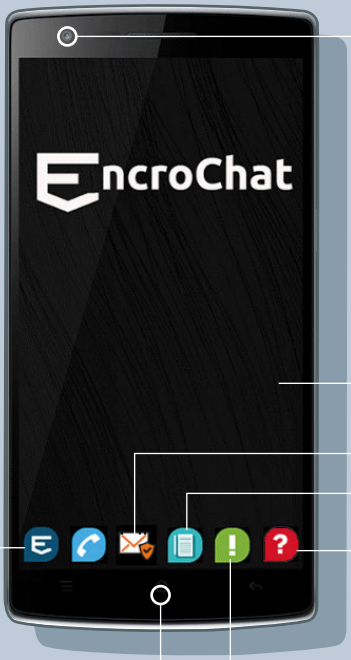
Under skalet på Encrochat



OMBYGGDA ANDROIDTELEFONER

Encrochat sålde telefoner där kamera, mikrofon och gps fysiskt kopplats bort för att förhindra att telefonen används för att spionera på ägaren. Röstsamtal krävde headset. Telefonerna var Androidtelefoner, bland annat från den spanska tillverkaren BQ.

EGNA SERVRAR

För att ytterligare öka säkerheten har trafiken skett via Encrochats egna servrar.

MODIFIERAT OPERATIVSYSTEM

Encrochat hade ett eget operativsystem, baserat på Android, men reducerat. Delar som kunde innebära säkerhetsrisker var borttagna. Det gjorde att apparna kördes i en säker miljö, där risken för attacker från annan programvara var liten.

ETT FÅTAL APPAR

Telefonerna har haft ett fåtal appar. Tre för krypterad kommunikation – röstsamtal, chatt och e-post – samt en anteckningsapp. De har även haft en funktion för snabbradering: När polisen bankade på dörren kunde användaren utplåna all info i telefonen med en pinkod.

END-TO-END-KRYPTERING

Kommunikationen har varit ”end-to-end”-krypterad. Det innebär att den är krypterad hela vägen till mottagarens telefon, och inte kan läsas av den som tillhandahåller tjänsten. Så fungerar även exempelvis Whatsapp, men inte Facebook.

SÅ KNÄCKTE POLISEN ENCROCHAT

Polisen upptäckte att Encrochat hade servrar i Frankrike. Antagligen manipulerade polisen servrarna så att ett spionprogram följde med en uppdatering till alla användare. Därmed fick polisen tillgång till Encrochats kommunikation i okrypterad form. Dessutom saboterades snabbraderingsfunktionen. Avlyssningen pågick i månader, fram till juni 2020.

ORGANISERAD BROTTSLIGHET

Encrochats kunder fanns i huvudsak inom organiserad brottslighet. Tjänsten lades ner i juni 2020. En liknande tjänst, Sky ECC, har nyligen också stängts. Det finns även en laglig marknad för säkra mobiltjänster, där användarna är till exempel beslutsfattare, säkerhetstjänster och kändisar. Liknande tjänster är viktiga för dissidenter i länder med auktoritära regimer.

KÄLLA/FAKTAKOLL: PONTUS JOHNSON, PROFESSOR I NÄTVERK OCH SYSTEMTEKNIK, KTH

Forskning & Framsteg