A Real-World Law-Enforcement Hack: The Case of Encrochat

Martin R. Albrecht[1], Sunoo Park[2], Michael A. Specter[3], and Douglas Stebila[4]

[1]King's College London, UK, martin.albrecht@kcl.ac.uk
[2]New York University, USA, sunoo.park@nyu.edu
[3]Georgia Tech, USA, specter@gatech.edu
[4]University of Waterloo, Canada, dstebila@uwaterloo.ca

25th June 2026

Abstract

In 2020, a coordinated law-enforcement effort infiltrated Encrochat, an end-to-end encrypted service provider, exfiltrating historical and real-time data and metadata over months. Encrochat was used extensively by organised crime, and the data from the operation was used as supporting evidence in over 6,000 arrests and related prosecutions across Europe. Encrochat's architecture was vertically integrated, with the company acting as both a device vendor and service provider; Encrochat sold modified Android smartphones with its own PKI and custom applications, including encrypted messaging based on the Signal protocol. In this work, we give the most detailed public account to date of Encrochat's infrastructure and how it was compromised.

An abridged version of this paper appears in the proceedings of *Advances in Cryptology – CRYPTO 2026*, © IACR 2026. This is the full version.

Contents

1 Introduction **3**

2 Preliminaries **4**
2.1 Android security 4
2.2 Related work 5
2.3 Other known law-enforcement compromises 5
2.4 Dramatis personae 6

3 Methodology and sources **7**

4 Encrochat system overview **9**
4.1 Infrastructure 11
4.2 Encrochat's Android 12
4.3 TLS certificates 13

5 Compromise **13**
5.1 Potential earlier compromises 14
5.2 Server compromise 14
5.3 Device compromise 17
5.4 The malware 26
5.5 Interpretation 28

6 Open problems in cryptography **29**
6.1 Subversion of cryptography 29
6.2 Covert adversaries 30

7 Legal context **31**
7.1 Extent of criminal use 32
7.2 Use of the evidence in prosecutions 33

A Subdomains **48**

B Virtual machine and host names **50**

C Extracted APKs **53**

1 Introduction

Cryptography, and information security more broadly, routinely assumes state(-level) adversaries. This, on the one hand, is justified by these attackers being the most powerful plausible adversaries, i.e. ruling out attacks by these adversaries rules out attacks from any adversary. On the other hand, nation-state adversaries have been shown to attack widely used information security and cryptographic mechanisms.

In particular, following the Snowden revelations, the widespread adoption of end-to-end encrypted (E2EE) messaging is one of the great cryptographic accomplishments of the past decade. Building on the foundation of earlier tools like Off-the-Record messaging [BGB04], applications such as Signal [CCD+20], WhatsApp [ADJ25], Apple iMessage [GGK+16, BS20] and Google Messages are now used by billions of users daily, and there are many other tools targeting specialised user bases: activism, journalism, healthcare, finance, nonprofits and more. Critically for this work, there have also been a series of bespoke solutions targeting organised crime, such as Ennetcom, ANOM, SkyECC, Ghost and Encrochat (§2.3).

Prior academic work has studied E2EE messaging from a variety of perspectives, including designing protocols and systems, developing security models and analysing existing protocols, and discovering flaws in designs or implementations. Our work complements this existing literature with a detailed chronicle of a real-world nation-state compromise of a deployed E2EE messaging system – the Encrochat hack – where the attackers used both technical means (malware) and more traditional policing tactics (warrants, court orders, seizures) to target all users of the system over months. Studying such a case is instructive for designing threat models and security definitions to resist attacks by advanced adversaries beyond the narrow setting of this particular compromise.

Encrochat. Encrochat was an organisation, operating from approximately 2013 to 2020, that offered modified Android phones and subscription services to select customers primarily in Europe. One of the main applications on the phone was a one-on-one end-to-end encrypted chat application based on the Off-the-Record (OTR) and Signal protocols. The devices had several design features to enhance security and privacy, including pseudonyms, disappearing messages, tamper detection, full disk encryption and remote and local wipe features. Encrochat devices were only available from certain retailers, and appear to have been widely used by and marketed to organised crime. By 2020, Encrochat had around 66,000 users.

Law-enforcement infiltration. In early 2020, after years of preparation, French and Dutch law enforcement, in collaboration with Europol, successfully breached Encrochat. After obtaining and decrypting snapshots of Encrochat's virtual machine-based server infrastructure, law enforcement deployed a malicious software update to Encrochat handsets, enabling them to collect stored and real-time data from devices. The information collected was shared with other European law enforcement agencies. In a synchronised operation starting in June 2020, police in multiple countries arrested more than 6,500 people, seizing hundreds of millions of Euros worth of cash, drugs and weapons, and disrupting kidnapping and murder plans [Goo23, EE20].

The Netherlands and the UK described it in official press statements as the biggest ever law-enforcement operation in their respective countries [Nat20, dM20],[1] Europol announced that the data obtained unlocked "access to unprecedented volumes of new evidence to profoundly tackle organised criminal networks" [EE20], and France noted that "some of the world's most wanted criminals have been identified" and that "the scale of the results ... allows the [French] gendarmerie to shine" within

[1] Further, the UK's *Integrated Review of Security, Defence, Development and Foreign Policy* 2021 claimed "a significant breakthrough in the fight against SOC in June 2020, when we infiltrated the encrypted communications of criminals ..." [UK 21]. It was well established already in 2021 that the UK did not infiltrate Encrochat, but that this was a French and Dutch operation.

Europe and internationally [dac20].[2]

Contributions and roadmap. In this work, we construct the most comprehensive public account to date of the Encrochat system and compromise. Despite some vocal calls for more transparency (e.g. [vLBM+22]), many details of the Encrochat hack have been kept secret due to ongoing legal proceedings across Europe and because certain aspects are classified under French law. Our research involved collecting and analysing more than 3,000 pages of documents from varied public and non-public sources (§3). Even so, many details remain unclear; we also present a systematic account of remaining gaps.

Beyond the preliminaries in §2 and our methodology in §3, our central contributions are: (a) §4 and (b) §5 give the most complete public account to date of the Encrochat system and law-enforcement operations respectively, covering details not previously reported; (c) §6 formulates some open problems for cryptography; and (d) §7 gives an overview of some of the legal context and controversies surrounding the Encrochat cases, geared for a technical audience.

2 Preliminaries

2.1 Android security

The Android Framework. Android is defined by the Android Compatibility Definition Document (CDD) [Andc], which specifies a number of APIs and structures, and any OS meeting the CDD can run most Android applications. Google provides a reference implementation of the Linux kernel and userspace framework that fulfils the CDD, which OEMs like Samsung customise to provide extra features, behaviour and hardware support. To market as "Android", devices must pass Google's test suites and comply with the CDD, enforced via Google's trademark on Android [MSB+23]. Most also run Google software such as Play Services and Chrome, though this is not a requirement. Encrochat avoided Google's branding and vetting, so may have altered the reference implementation. We cannot confirm such changes, but Encrochat at least started with a CDD-compatible implementation used on their devices [Gre22].

Android updates. By default, Android apps (APKs) include a cryptographic signature and a certificate with the public key for verifying the package. Android's package manager `pm` does not verify certificate chains – there is no Certificate Authority infrastructure – and on update, apps must use the same certificate as the installed version; otherwise, they install as new apps [Andb].

Update distribution varies by OEM. Typically, OEMs send device-wide updates to Google via the Over-the-Air (OTA) update process, though updates can also start via third-party services or on-device files. Updates ('packages') are shared as signed zip files, verified using a certificate pre-stored on-device. Any updated APKs must also be signed to meet the `pm` update requirement. Looking ahead, we note that it would be difficult to modify the Android reference implementation to avoid signing updates.

Android application security. Android uses containment techniques to run multiple apps safely, based on each app's signature verification key. Each app runs as a unique user with isolated file system access via SELinux and Linux filesystem permissions tied to a UID derived from the APK's certificate. Apps sharing the same certificate can access each other's data. Most apps run in the restricted `untrusted_app` SELinux container, relying on interprocess communication with privileged system apps for sensitive resources like location or camera. Access is controlled through a fine-grained permissions system. OEMs may create platform-signed apps – e.g. settings or AI assistants – using the same key as the system image. These run in more privileged SELinux environments

[2] Translated from the original French.

(e.g. `system_app` [Anda]) and have broader filesystem access, enabling direct hardware access and bypassing OS permissions checks.

2.2 Related work

Prior academic literature on Encrochat has focused primarily on legal issues and appeared in law venues largely in Europe. For example, Theune discusses the sufficiency of the evidence upon which the Encrochat operation was authorised [The21]. Griffiths and Jackson [JG22, GJ24] discuss the admissibility of Encrochat evidence in UK cases and argue for transparency-enhancing reform. Stoykova [Sto23] critiques the operation's secrecy in relation to a right to a fair trial. Oerlemans and van Toor [OvT22] examine human rights issues around the Encrochat cases with a Dutch focus. Sagittae [Sag23] discusses the operation's lawfulness in various European jurisdictions. Many works also discuss the complexities of this large multi-jurisdictional operation. This list is not exhaustive.

The compromise of Encrochat fits into a long list of compromises of dedicated secure communication platforms with specialised phones, many connected with organised crime (overviewed in §2.3). Scholarship in law and other fields has also studied some of these (see §2.3), as well as law-enforcement hacking more broadly (e.g. [May17, Das20, PC17, Buc20]).

The focus of our work, in contrast, is on how the Encrochat phones and the law-enforcement operation and compromise worked from a technical computer-security perspective. The technical and legal aspects are intertwined, as further contextualised in §7: the technical details bear upon some of the key legal issues in the Encrochat cases, and the way the operation was conducted was influenced by legal frameworks in France and other involved jurisdictions in noteworthy ways.

This work follows in the tradition of a number of works that examine government efforts as related to cryptography. These include analyses of government proposals on key escrow [AAB+15, AAB+97, Bla94], government attacks on encrypted systems [CMG+16], and measurement studies [ABD+15] of the same. Though similar events to Encrochat's have occurred (e.g. the FBI's Operation Trojan Shield [FBI25] and the Athens Affair [PS07], and others in §2.3), we are not aware of prior formal analysis or documentation of these.

There is also prior work overlapping criminology that has examined policing crime chat networks with a focus on Encrochat [Pfe24] and police misconduct in the context of Encrochat and other investigations [Hut25].

2.3 Other known law-enforcement compromises

The compromise of Encrochat fits into a long list of compromises of dedicated secure communication platforms with specialised phones, allegedly used by and marketed to organised crime groups. A timeline of many such examples is given by [Oer24b]. Some notable examples include:

Ennetcom was shut down in 2016. Reportedly, officials in the Netherlands were able to decrypt many communications by Ennetcom users, "likely because the company had housed decryption keys on the same server where it stored messages" [Cae20, HvW23].

PGP Safe was shut down in 2017 and prosecutors reportedly downloaded keys to decrypt PGP-encrypted messages [Oer21].

IronChat was shut down in 2018 and Dutch investigators reported to have decrypted about 2^{18} messages [Goo18, HvW23].

SkyECC was compromised by Dutch law enforcement, who intercepted about a billion messages and decrypted about half of them between 2019 and 2021. In particular, a 2018 report by investigators identified the location of Sky ECC infrastructure in the OVH datacentre in Roubaix, France. In the same year, a Dutch judge allowed an application to seize copies of the Sky ECC servers for technical research into encryption and interception of messages on the phone network. In 2019, a French

prosecutor at the Lille court initiated a formal investigation into Sky ECC. Also in 2019, a French prosecutor successfully applied for a court order to intercept, record and transcribe communications passing through Sky ECC servers in France. In December 2020, Dutch investigators reportedly worked out how to obtain encryption keys from Sky ECC handsets. Work began on decrypting a backlog of intercepted encrypted data. In 2021, French investigators began live interception and decryption of Sky ECC phones [Goo25, Sag23, OR23].

ANOM was a Trojan horse distributed by the United States Federal Bureau of Investigation (FBI) and the Australian Federal Police (AFP). It was operational between 2018 and 2021 [Cox24].

Exclu was shut down in 2023 and law enforcement read messages for five months prior [Oer25].

Ghost was operational between 2015 and 2024. It was infiltrated by the United States Federal Bureau of Investigation and the French Gendarmerie [Ske24]. Technical details on the takedown are scarce but reportedly some technical resources and developments were provided by the Internal Security Fund's Project Overclock.

MATRIX was shut down in 2024. For months, more than 2 million messages were intercepted by law enforcement [Oer24a].

2.4 Dramatis personae

We provide a brief introduction to some of the government, law enforcement and commercial entities that are mentioned in this work.

Government and law enforcement

Eurojust (the European Union Agency for Criminal Justice Cooperation) is an EU agency established to facilitate cooperation between member states, including on organised crime.

JIT (Joint Investigation Team) was a Eurojust working group set up between French and Dutch law enforcement to infiltrate Encrochat; UK law enforcement was invited to participate in the JIT.

Europol is the European Union Agency for Law Enforcement Cooperation: The law enforcement agency of the European Union, which supported the JIT.

Gendarmerie Nationale is one of two national law enforcement agencies in France, whose remit includes cybercrime via the C3N.

C3N (Centre de Lutte Contre les Criminalités Numériques) is a service within France's Gendarmerie Nationale focused on cybercrime, which led France's participation in the operation.

STNCJ (Service Technique National de Captation Judiciaire) is a French government agency which developed parts of the malware used to infiltrate Encrochat.

NCA (National Crime Agency) is the UK's national law enforcement agency, whose remit includes organised crime and cybercrime.

Douai Court of Appeal (Cour d'Appel de Douai) at the Lille Judicial Tribunal (Tribunal Judiciaire de Lille) is a regional court which issued several orders authorising C3N's operation.

Operation Emma is a codename for the French operation.

Operation Venetic is a codename for the UK operation.

Technology providers to Encrochat

OVH is a French cloud computing company whose data centre in Roubaix, France, was used to host Encrochat services.

KPN is a Dutch telecommunications company which Encrochat contracted to provide mobile connections and SIM cards for Encrochat devices.

Gandi SAS is a French DNS registrar and service provider, one of several used by Encrochat.

DNS Made Easy is a DNS service provider, one of several used by Encrochat.

Hostpoint AG is a Swiss DNS registrar and service provider, one of several used by Encrochat.

Cloudflare is a US content delivery network and DNS service provider, one of several used by Encrochat.

3 Methodology and sources

Our analysis proceeded largely through an iterative and reflexive content analysis of documents. Reflexivity here refers to interactive discussions amongst the authors to resolve questions and ambiguities arising from the data. While some authors have experience doing qualitative-coding-based research, we highlight the limitation that no author is trained in the coding of 'messy' research data [Cha06].

Each source document (or a translation) was reviewed by at least two authors. The main source languages were English, French and German.[3] Many sources that originate from France were also available to us in English translations for use in UK court cases. In this section, we cite both originals and translations; in the rest of this work, we cite English translations rather than the originals, unless noted otherwise. We reviewed some other non-English documents through automated translation to English. We were able to correct ambiguities and inconsistencies in translations of French and German documents by referring directly to the originals, as some of the authors can read French and German. We also refer to a few sources in Dutch, Spanish, and Italian, for which we used automated translations to English.

Throughout this work, we treat the statements in these documents as reflecting the genuine understanding of their respective authors. That is, we assume the evidence available to us might be factually wrong or unreliable, but is not deliberately falsified. Sometimes we identified ambiguities or conflicting information, which we indicate where relevant throughout this work.

Publicly referenceable sources. We relied on publicly referenceable information from several different classes of sources, including:

- the eight warrants in both English translations and French original [Nor20a, Nor20c, Lec20a, Lec20b, Nor20b, Nor20d, Mor20a, Mor20c, Har20a, Har20b, Mor20b, Mor20d, Ale20c, Ale20e, Ale20a, Ale20d] granted by the Douai Court of Appeal in Lille, France, between January and June 2020, authorising the law enforcement operation (the English versions were translated by unknown authors and were used in the UK court system);[4]
- UK, French, and German court documents, particularly rulings (e.g. [Liv21, Inv23, Lan21, Bun22]);

[3] Our research team includes native proficiency in English and German, and advanced French comprehension.

[4] We have verified the correspondence between French originals and English translations for all warrants. Although for simplicity, we may cite just one version, we have verified any references to these warrants in this paper in both language versions.

- historic DNS, WHOIS, and certificate data for domains used by Encrochat (e.g. [Dom24, SWI24, Sec23]);
- media reporting on Encrochat, including multiple articles by William Goodwin for Computer Weekly [Goo21, Goo22a, Goo22b, SG21], Joseph Cox for Vice.com [Cox20a, Cox20b, Cox21a, Cox21b, DC22], and Alexandra Posadzki and Joe Castaldo for The Globe and Mail [PC24a, PC24b];
- Encrochat marketing materials on the Internet Archive [Enc15, Enc19a, Enc19b, Enc19c].

Other sources. We reviewed additional documents, some of which are referenced in publicly available sources (including those above),[5] and some of which may have been available on the public Internet in the past. These additional sources were mainly statements and evidence submitted in court proceedings, including:

- warrant applications from the French court system [Dec20e, Ber20a, Ber20c, Ber20d, Dec20a, Ber20k, Ber20g, Ber20j, Ber20f, Ber20l, Ber20h, Dec20b, Ber20i, Ber20e];
- a request for technical assistance to the STNCJ [Dec20f],
- reports of successful compromise [Dec20c, Ber20b],
- expert witness reports by Ross Anderson [And22a, And22b] and Kushvinder Raheloo [Rah23] (for defendants) and IntaForensics [Int21] (for the prosecution) in UK court proceedings;
- statements submitted in UK and French court proceedings by Jeremy Decou, a law enforcement officer in the C3N [Dec20d, Dec21b, Dec20e, SD20];
- expert witness reports in UK court proceedings by members of the National Crime Agency [Ave21, Shr21e, Shr21a, Shr21b, Shr21d, Shr21c];
- a joint expert report by expert witnesses Luke Shrimpton and Duncan Campbell (for the prosecution and defence, respectively) summarising agreement and disagreement [SC22];
- transcripts of UK court proceedings [Fae22];
- notes from law enforcement meetings (e.g. Europol [Eur20a, Eur20b, Eur20c, Eur20d] and law enforcement emails [NCA20a, Lau20, Jak20a, Jak20b, SD20, Swe20], disclosed in UK court proceedings).

To our knowledge, these documents are not currently available to the public. We have: (1) confirmed the authenticity of each of these sources with at least one person familiar with the proceedings; (2) wherever feasible, cross-referenced and verified information provided across publicly available sources and other sources; and (3) communicated with a number of individuals familiar with the Encrochat cases, and cross-checked our understanding of Encrochat and its compromise with what we learned in these communications.

We favour citing public sources wherever possible, and recognise that this supports open science. When we cite a source, we may not include all corroborating non-public sources alongside. Many of the sources that we reviewed contained similar or overlapping material. While we took into account the agreement between these materials in evaluating how well supported our understanding is, we opt to cite a smaller number of selected sources that we find credible and representative, favouring public sources, rather than to enumerate all corroborating sources in every instance. For example,

[5]Thus, the provision of multiple references should not necessarily be understood as the provision of multiple independent sources.

in the case of expert witness reports, we often cite only the most relevant or detailed expert report for a given statement, even if the statement is corroborated by multiple expert witnesses.

Wherever we are aware of any inconsistency or disagreement between different sources on a point discussed in the paper, we note it explicitly. That is, unless otherwise noted, any statement in this paper with a citation may be regarded as *primarily supported* by the cited source(s), and moreover *not inconsistent* with any of our sources, public or otherwise.

Finally, we note that the warrants and warrant applications begin early in the Encrochat operation, and span most of the operation's duration, as extensions and expansions of authorisation were requested and granted. See §5.3.

Ethics considerations. Our study was exempt from IRB/ethics review processes in most of our institutions (it is not human-subjects research), but ethics approval was sought through King's College London (KCL).

A first application for "data collection [...] presenting sensitive issues" covered "reading court documents (which may contain defendants' personal information) and public documents such as press reporting." This application considered risks due to secrecy laws: "By pulling information together from disparate databases, inferences may be made, whether explicit or implicitly to those with the technical knowledge of how the attack was facilitated. We therefore need clarification on the ethics of proceeding with this research and ... mitigations." KCL approved this subject to a risk assessment being approved by the Head of Department and the Research Governance Office's sign-off. Both did take place.[6]

We had discussions with qualified lawyers in two key jurisdictions and additional more informal discussions with legal experts in several jurisdictions, including on potential legal risks to parties involved in criminal proceedings, our sources, other stakeholders and to ourselves. Based on these discussions and consultation with sources, we determined that the risks are likely limited, and the benefits of the research justify pursuing and publishing it. Our sources are comfortable with what we have chosen to publish. Due to the sensitivity of the topic and out of an abundance of caution, and to respect their wishes, we keep many of our contacts anonymous and generally do not directly reference our conversations with them.

Some aspects of the Encrochat operation are covered by French national defence secrecy laws, as discussed in §7. We have never had any access to, or tried to gain access to, any materials that are classified as French national defence secrets.

4 Encrochat system overview

Encrochat was a communications provider that sold modified Android phones that supported end-to-end encrypted communication. Through its lifetime various Android phones were used,[7] but in 2020 the BQ Aquaris X2 was reportedly the predominant model [Cox20b] with the BQ Aquaris X3 slowly taking over [Ale20a]. While some sources refer to all Encrochat phones as "carbon units", e.g. [Esk20], the term is reserved for BQ Aquaris X3 devices in the technical documents we have examined.[8]

At the time of its shutdown Encrochat had 66,134 accounts (registered SIM cards) [Bun22, ¶11]. Encrochat devices were used in the Netherlands, Spain, the UK, Germany, Italy (in that order of number of users per country) [Bun22, ¶11] and other countries, like France (ranked 13th) [Lan21,

[6] We made a second application at KCL for interviews, covering additional non-public information. We obtained self-cert approval per KCL policy. We did not end up conducting interviews, partially due to interviewee anonymity concerns. We did not make similar applications at other institutions, after abandoning our interview plans.

[7] "OnePlus One, OnePlusX and BQ Aquaris X" [Bun22, ¶8], see also e.g. `https://community.oneplus.com/thread/470818`

[8] See also `https://fccid.io/2AN87CARBON` and `https://fccid.io/2AN87CARBON/User-Manual/User-manual-4663716.pdf`.

¶104]. Encrochat devices could only be purchased from resellers [Enc19b][9] and not on the Encrochat website[10], with devices selling for about 1,600€ on eBay including a six-month subscription [Bun22, ¶10]. Subscriptions cost about 1,500€ per six months and included 24/7 support [EE20].

Top-level domains used by Encrochat included `encrochat.ch`, `encrochat.network`, `encrophone.com`, `esocrypt.com`, and `encrochatsure.com`.[11] From 2020, it also used the domain `zerolegacy.ch` [Ale20a].

A company behind Encrochat was registered in 2014 [Gal20]. It was claimed in [Gre22] that the ownership of Encrochat changed to an unknown entity in 2016 [Gre22]. This claim conflicts with other evidence [Cox21a, DC22, PC24a, PC24b].

Encrochat phones had some combination of the GPS, microphone, camera and USB ports physically disconnected [EE20].[12] Some debugging facilities, such as Android Debug Bridge and recovery mode [Bun22, ¶8], had been removed to harden the devices against forensic examination [And22a, Som21].[13]

Encrochat phones were dual boot. The default boot OS was a dummy Android system with essentially no functionality [Liv21, ¶4], which could then be rebooted into a password-protected partition running the Encrochat operating system. The Encrochat OS used full disk encryption, reportedly utilising the phone's trusted platform module (TPM), but details are unclear.[14] At least at some point, the Encrochat OS was claimed to be based on the "Guardian ROM" [Gre22].[15]

Encrochat devices offered a kill switch, allowing users to wipe the device when entering a certain PIN or when a certain number of password attempts were unsuccessful [Cox20b, Enc19a]. Users could also remotely wipe their devices [Enc19a]. Encrochat servers had the ability to switch off handsets [Som21]. The device performed some tamper-detection checks during boot [Enc19a].

Encrochat devices offered three main applications:

- *EncroChat.* A one-on-one[16] end-to-end encrypted chat application, whose traffic was routed through one or more Encrochat servers in France [Liv21, ¶9],[17] offering disappearing messages (user controllable, but the default expiry time was seven days [Liv21, ¶5,¶73]). The Encrochat marketing material [Enc19a] advertised this as OTR-based [BGB04]. In [Gre22] it is reported it was based on ChatSecure[18], which indeed relies on OTR. Several sources [Cox21b, Goo22a], in contrast,

[9] "The site states that Encrochat has resellers in Amsterdam, Rotterdam, Madrid, and Dubai" [Cox20b]

[10] While [EE20] claims that "Encrochat sold" the devices, we interpret this to mean through resellers.

[11] The use of `encrochatsure.com` seems to have stopped at the end of 2017, according certificate transparency logs: `https://web.archive.org/web/20231102165241/https://crt.sh/?q=encrochatsure.com`.

[12] While some marketing material, e.g. [EE20], claims all phones had their cameras disconnected, this does not appear to be accurate. First, law enforcement eavesdropped on pictures sent between Encrochat devices, suggesting but not necessitating that at least some phones had cameras. Similarly, at least old versions of Encrochat advertised an optional "Encrypted Camera function" that required a "physical back camera" [Enc15]. Indeed, technical reports discuss the camera functionality [Shr21c].

[13] "The EncroChat phones we have examined are modified Aquaris BQ X, 2X or 3X [[sic]] ('Carbon') devices. [[. . .]] The handsets also have their firmware modified to block the USB port and thus frustrate normal forensic tools. In the photograph below, I exhibit on the right a normal Aquaris X2 purchased on eBay, and on the left a phone believed to be supplied by EncroChat. The normal phone has a 'bq' seal on top of the screw holding down the USB port cover, below the battery on the picture; but on the suspected EncroChat device, this has been tampered with. The usual firmware mechanisms for putting a phone into emergency download (EDL) mode for forensic examination have been blocked, so to experiment with the phone we moved the motherboard of the Encro device to the unmodified device, and added a physical switch to force a hardware EDL boot." [And22a]

[14] "An Encrochat device can not be brute forced to mount the encrypted data partition. We generate an RSA public/private keypair with which the public key portion is combined with your disk encryption passphrase. Without the private key, which is in a hardware backed keystore, you can't mount the encrypted data partition" [Enc19a]. It is not clear to us why RSA would play a role in full disk encryption and why one would combine a password with the public key.

[15] See `https://web.archive.org/web/20231102165558/https://www.wilderssecurity.com/threads/guardian-rom-secure-android-os.348416/`.

[16] We did not find any mention of group-chat features; [Int21] suggests explicitly that group chats were not possible.

[17] But one Encrochat website referred to "[o]ur servers, located offshore in our datacenter . . . " [Enc19c]

[18] See `https://web.archive.org/web/20231102165716/https://github.com/chatsecure`.

report that it was based on Signal. This suggests the developers switched to Signal at some point in between. Throughout court documents we examined, all experts discuss Encrochat as Signal-based.[19] User handles were claimed not to be linkable to device or phone numbers. Encrochat users could only communicate with other Encrochat users [Liv21, ¶5].[20] It appears users could also delete messages on others' phones, presumably their own [Esk20, Law20]. A notary system facilitated contact verification, allowing users to introduce two of their contacts.

- *EncroTalk.* A ZRTP-based VoIP solution,[21] presumably to be used with an external headset [Cam21].[22]

- *EncroNotes.* A note-taking application which stored user notes locally in an encrypted database with its own user-chosen passphrase contained within an encrypted partition [Enc19a]. An optional server backup feature used two-factor authentication (IMEI and passphrase) [Enc19a].

4.1 Infrastructure

Encrochat's infrastructure included a number of services that supported Encrochat's business, development and operation. Unless otherwise cited, information in this subsection is based on [Rah23]. These services include:

- *Encrochat proxy and load balancer.* All communication with the servers went through a proxy server that allowed Encrochat to redirect particular devices and URLs to a virtual machine (VM). This provided both compatibility between device versions and support for load balancing [Exp25].

- *Update service.* Devices queried Encrochat's servers for both firmware and application updates.

- *Encrochat image server.* A supplementary service built into Encrochat's texting protocol that allowed users to share images.

- *Development & staging.* The developers followed many modern development practices, including the use of testing, production and development servers.

- *Full disk encryption.* All VMs used full disk encryption via LUKS, with keys stored in TANG key servers.

- *Billing & customer management.* Encrochat had several servers exclusively used for billing, customer management and customer assistance.

- *Marvin analytics server.* Encrochat phones included an application called *Marvin* which acted as a crash logging and performance analytics tool and uploaded reports to a central server.[23]

Fig. 1 depicts our understanding of Encrochat's network infrastructure. All servers were hosted by OVH, a Virtual Private Server (VPS) provider located in Roubaix, France [Nor20a, TT25]. §5.2 provides further details on these servers, and their involvement in Encrochat's eventual compromise.

Encrochat did not use Google's services or servers for distributing application and operating system updates. Instead, it used its own update servers, first at `update.encrochat.ch` and later also at `update.zerolegacy.ch`, as further discussed in §5. Encrochat did, however, use Google's DNS server `8.8.8.8` [And22a].

[19] "We observed experimentally that EncroChat uses the Axolotl version of Signal which has been obsolete since about 2015, but we have not been able to explore the extent to which even the original EncroChat app implements the Sesame protocol, which is used by Signal to manage message concurrency." [And22a]

[20] Earlier on, PGP support via the K-9 mail app [Gre22] was available to "transition from PGP" [Enc19a].

[21] ZRTP is a protocol for cryptographic key agreement for end-to-end secure VoIP. Details are available in IETF RFC 6189 [CJZ11].

[22] However, it seems this traffic was not intercepted or at least not used in criminal proceedings: "But we get no instances of this in evidence or disclosure" [Som21].

[23] "Marvin" is also used to refer to the Android Accessibility Suite, which is unrelated to "Marvin" in the Encrochat context.

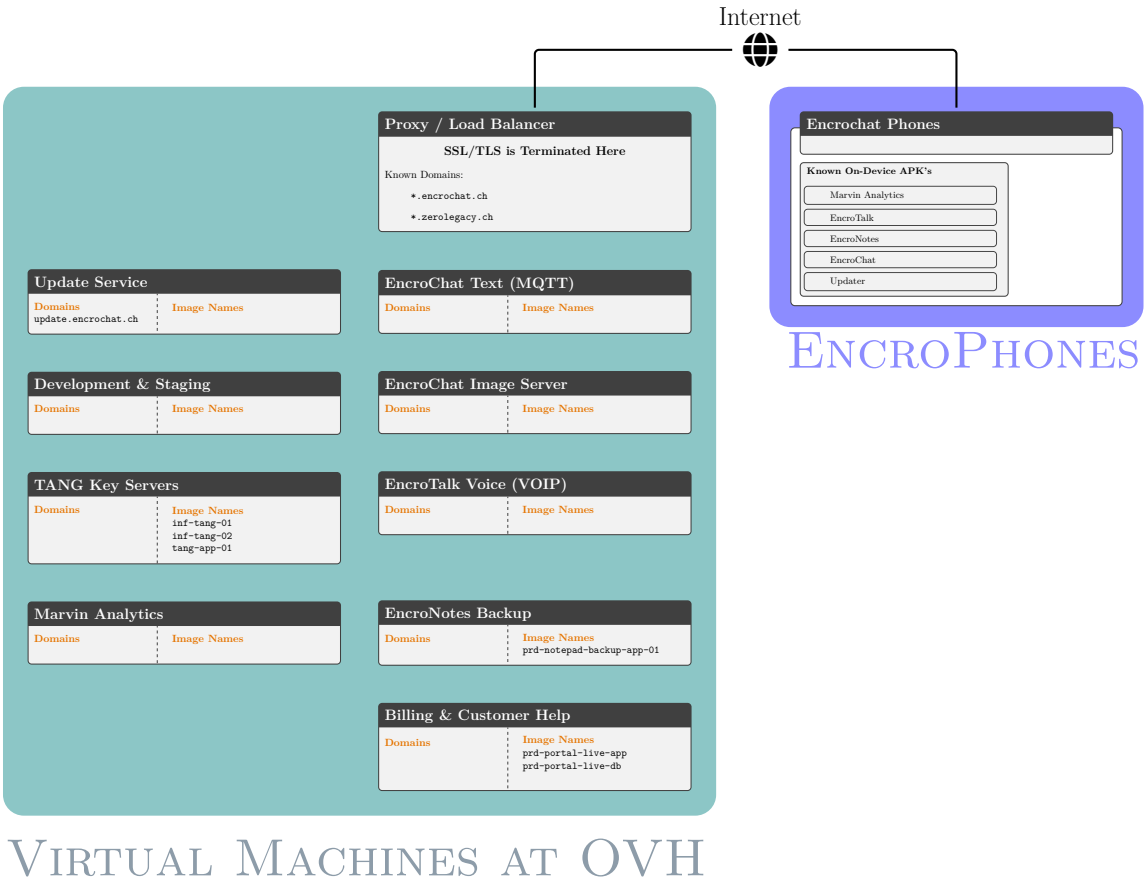

Figure 1: **Overview Diagram of EncroChat's Infrastructure As We Understand It.** This diagram only includes URL connections, services and linked VM image names whose use and link with other resources is explicitly confirmed by the source material. There are a number of other resources and network components not in Fig. 1, which are discussed elsewhere in this paper (e.g. the full list of VM image names in App. B).

4.2 Encrochat's Android

Encrochat's custom Android firmware shipped a mix of seemingly standard Android applications and several custom ones (see App. C). Three custom APKs are of particular interest to this work: the Admin, Marvin and Updater applications. Each of these were platform-signed applications, and therefore able to run as `system_app`, bypassing normal Android permissions checks [Rah23]. We describe the function of these applications below:

- *Admin.apk* provided mobile device management and settings control policies, including password timeouts and other information [Rah23].

- *Marvin.apk* was for analytics, error logging and crash reporting. It communicated only with `marvin.encrochat.ch` [Rah23].

- *Updater.apk* downloaded and installed updates from `update.encrochat.ch` for all applications and the firmware-level OTA update package; it could also remove arbitrary programs from the device. Remarkably, all operations occurred silently – the application did not query or alert the user before installing updates or removing applications [Rah23].

Encrochat devices regularly polled the server for software updates [Bun22, ¶16]. The custom OS also restricted devices from communicating with services outside of Encrochat's control. This was implemented by removing other root certificates from the Android trust store, leaving only Encrochat's own custom root certificates [Rah23], and, following the Android security model [MSB+23], the Encrochat system applications (Admin, Marvin and Updater) were signed by the platform key. The Updater APK used certificate pinning to ensure it was communicating using a previously used certificate [Rah23].

4.3 TLS certificates

Encrochat ran its own certificate authority (CA) for the subdomains of `encrochat.ch` and `zerolegacy.ch`. Censys.io holds a CA key for "EncroChat Root CA" in its database, valid from 11 February 2015 until 29 June 2042.[24] The same database contains TLS host certs signed by this CA for the `encrochat.ch` subdomains `activate`, `billing.talk`, `connect`, `connect.talk`, `currency`, `marvin`, `media.im`, `notes`, `simple`, `stargate`, `status`, `update` and `vanc`.

TLS host certs for `helpdesk.encrochat.network`, `cas.encromail.ch` and `push.field.bios.run` and `*.field.bios.run` are also present; see Table 1. The last two are valid from 24 March 2017 and 7 April 2017 respectively and valid for 10,000 days. These may have been used to sign application updates, as indicated by their `Organizational Unit` (OU) fields being set to "`apps`". The two directors of Binary IO Solutions Inc. are said to have been involved in the development and running of Encrochat [PC24a, PC24b].

As noted in §2.1, Android does not use a public-key infrastructure (PKI) or CA hierarchy for application signing. Thus, the standard Android package manager would ignore signatures by "EncroChat Root CA".

Table 1: Notable common names signed by the "EncroChat Root CA" key.

CN	ST	C	O	OU
`helpdesk.encrochat.network`	Panama	PA	EncroChat S.A.	Web
`helpdesk.encrochat.network`	Panama	PA	EncroChat S.A.	web
`cas.encromail.ch`	Panama	PA	EncroChat S.A.	cas
`*.field.bios.run`	BC	CA	Binary IO Solutions Inc.	apps
`push.field.bios.run`	BC	CA	Binary IO Solutions Inc.	apps

Similarly, we can find a "ZeroLegacy.ch Authority"[25] and a "Zero Legacy Intermediate CA" key[26], valid from 16 and 15 February 2020 respectively, and valid for 3650 and 365 days respectively. The former signed `zerolegacy.ch` subdomains `*`, `a1`, `*.a1`, `*.a2`, `billing.talk`, `currency`, `simple`, `connect`, `media.im`, `update`, `notes`, `connect.talk`, `status`, `marvin` and `stargate`.

5 Compromise

In this section, we report how Encrochat was compromised by law enforcement. Fig. 2 provides a graphical timeline of key points.

[24] See `https://platform.censys.io/certificates/66c70d229b80b4f95b6af4cc19c2e4a0cdf0ff7bea72c4907ef6a2bdeb0b3043`.

[25] See `https://platform.censys.io/certificates/776df9041f0d693c99a3536caaf803859ad3c6a6fb5cec25767dbea663bc63a2`.

[26] See `https://platform.censys.io/certificates/56ec57e7d02501db7b2f8f1fc310e60588128da93c78bae17cdde273f8f3cfed`.

Entities. We reference many government and commercial entities in this section, sometimes by acronym only; see §2.4 for a listing of entities.

Notation. This section includes a number of quotations that include square brackets in the original. In this section only, we use double square brackets to denote our own insertions and replacements; any single square brackets in quotations may be assumed original. Other sections use the common convention of single square brackets to denote our insertions and replacements.

5.1 Potential earlier compromises

Some reports assert that law enforcement had infiltrated Encrochat as early as 2016. In 2016 an alleged "whistleblower" claimed Encrochat was working "with the NSA and FBI, due to warrants being issued demanding access to their Canadian & Amsterdam-based servers" [Nic16a].[27] The accusation was vehemently denied [Gre22]. We are not aware of any evidence substantiating this accusation.

A blog post dated March 2016 [Nic16b] reported to have identified several practically-exploitable vulnerabilities in Encrochat: (a) The PGP-encrypted e-mail client did not sanitise e-mail header metadata properly and leaked IP addresses; (b) the shipped version of OpenSSL was still vulnerable to Heartbleed and (c) the Encrochat servers used self-signed certificates and thus were open to machine-in-the-middle attacks.

A witness for the UK National Crime Agency (NCA) gave evidence to the UK Investigatory Powers Tribunal that the NCA had obtained "a TLS encryption key, which was needed to 'spoof' the Encrochat server" [Goo22a] in 2018.[28] This is compatible with the beginning of "Operation Emma" discussed at length below, which was granted permission to copy the Encrochat servers in December 2018 [Bun22, ¶11] and [Nor20a]. However, the copying only commenced in January 2019 [Lau20, Cae23]. Furthermore, the same witness also disclosed that the NCA had "access to images of Encrochat servers towards the end of 2018 that had not been supplied to the NCA by the French police" [Goo22a],[29] refusing to disclose the source because it is "sensitive".[30] Finally, the same witness reportedly worked on their own attack/implant but abandoned their efforts when French law enforcement got in touch [Goo22b].

5.2 Server compromise

November 2018. French law enforcement, specifically the public prosecutor in Lille and C3N, began an investigation into Encrochat as a criminal enterprise itself [Bun22] on suspicion of a criminal

[27] Until 12 December 2018, Encrochat also had servers in Amsterdam [TT25].

[28] TLS 1.3 was only standardised in 2018, so TLS use in 2018 would have predominantly consisted of TLS 1.2 or earlier, in which RSA keys could be used for both signing and key transport.

[29] "Q. And towards the end of 2018, you had access, didn't you, to a server image? A. Correct. Q. And that was a server image that had not been supplied by the French authorities? A. Correct." [Fae22]

[30] These images may have been discussed in a UK meeting on 8 January 2020: "Several meetings between NCA and French Gendarmerie have failed to obtain the encrochat downloads on police-to-police basis. No specific reason given for this at meetings held [[. . .]]. A copy given [[redacted in source]] due to good working relations between technical officers however this may have been informally. No updated versions apparently given [[redacted in source]]. Impasse between NCA and French Gendarmerie and cps liaison assisted at meeting where it was discussed as to how to get over the problem. At that time, the view was that EIO not appropriate. No specific reason given by French for non-provision of download. Dutch have downloads (multiple downloads of Encrochat have been taken) after an EIO. Potentially further copies of server are now available, one such update is known of. French appear to be getting updated servers downloads. This download captures the whole of Encrochat at a given time so new updated downloads would be needed to be obtained whenever the French get them. Dutch investigation is understood to be good in relation to download." [Jak20a] In July 2018 Dutch investigators reportedly "took a look" at the servers in France [TT25, our translation]. Moreover, as mentioned above, until 12 December 2018, Encrochat also had some servers in the Netherlands [TT25]. This may or may not be the source of these British server images.

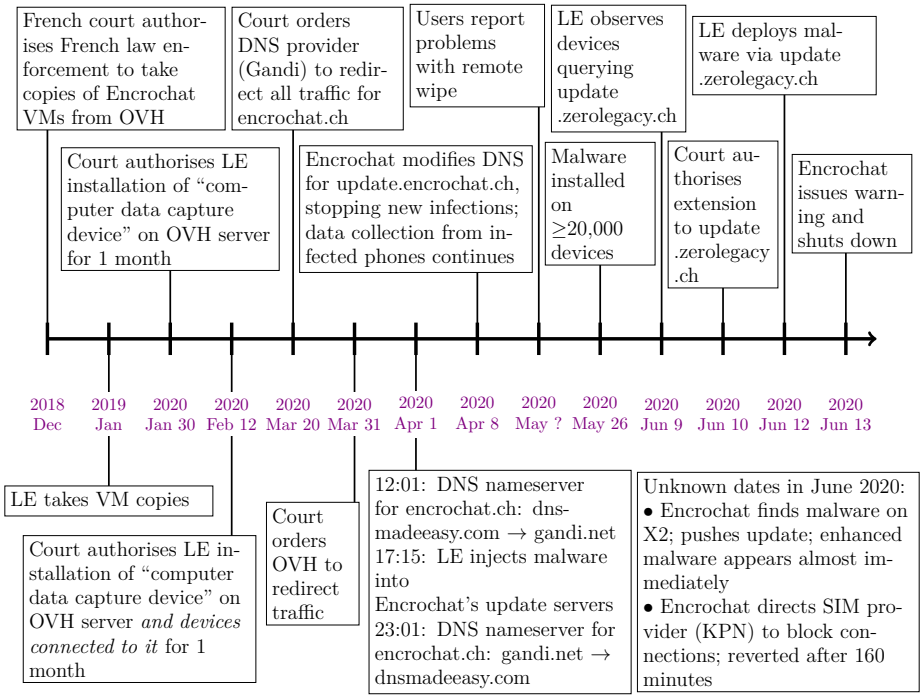

Figure 2: Timeline of key events

organisation for the commission of offences punishable by ten years' imprisonment (in particular, the crime of trafficking in narcotics) and for circumventing French cryptography regulations [Nor20a].[31]

December 2018, January 2019 and October 2019. A French court authorised C3N to take copies of the Encrochat virtual machines hosted in Roubaix, France, in December 2018 and October 2019 ([Bun22, ¶11] and [Nor20a]). As mentioned above, the actual copying took place in January 2019 [Cae23, Lau20]. A second copy took place in October 2019 [Lan21, ¶103].[32] Specifically, the targets were the servers hosting `encrochat.ch`. The recovered data consisted of "static image of the virtual machines' contents making up the ENCROCHAT system at this stage." [Nor20a].

Development servers. It is plausible that Encrochat kept a development environment in the data centre in France – including application signing keys. "[[A]]ccording to one expert" the images covered a "development server, where new code is created and tested" [Cae23]. Similarly, the warrants state that "the virtual private network server for the initial configuration of the BQ devices (programming of the Encrochat system)" [Nor20a] was copied. An expert witness wrote "We read that the JIT identified and copied both the development server and the update server. The former presumably had the EncroChat source code and tool chain [[. . .]]" and "The NCA officers record 'seizure of development server', which appears to imply access to the source code and development environment for the Encro apps on the handsets and perhaps also for the code used to customise Android (e.g. to set up the hidden partition and to block software access to EDL mode)" [And22a]. A note titled "EuroJust Meeting 22/01/2020" contains the notes "[[redacted in source]] servers —

[31]The Encrochat cases' overwhelming focus is on the drug trafficking charges, not the use of cryptography. §7 provides more discussion of French cryptography controls and their role in the prosecutions based on Encrochat data (see Footnote 82).

[32]"[T]he copies of the Encrochat servers were [[. . .]] performed [[. . .]] in January 2019 and October 2019 ; a new one will be done shortly" [Lau20]

development servers? May have passwords, keys etc ... " and "Need to take down development servers also" [Swe20]. Similarly, meeting notes titled "JIT MEETING Notes 22.1.120 Eurojust The Hague — 9-2pm" contain "French presentation: [[...]] Technicians have servers in [[redacted in source]] which are for development and not of use. Interested in getting that data." and later "France: Development servers [[redacted in source]]" [Jak20b]. Indeed, according to [Ave21], virtual machines with names such `dev-docker-test-box`, `dev-themeapp-01`, `stg-activation-activation-app-01`, `tst-bshd-01`, `tst-crypto-migration-app-01` and `tst-vm-01` etc. were identified (see App. B).

An alternative interpretation could be that Encrochat hosted their revision control server in the OVH data centre and used some Continuous Deployment solution, which would also explain the presence of software-update signing keys on these servers, as presumed in [And22a]. However, the VM names mentioned above suggest the former interpretation.

Full-disk encryption and keys. The haul contained mostly full-disk encrypted virtual machines, but also unencrypted ones [Lan21, ¶104], including two TANG servers [Nor20a], used to store and manage encryption keys for clevis[33] which can be used to provide key material to LUKS-type full-disk encryption during boot. Virtual machines called the clevis service to gather key material for decryption, which in turn queried the TANG servers (`inf-tang-01` and `inf-tang-2` [Nor20a]).

Law enforcement extracted keys from the unencrypted TANG servers, which served as a pivot point to decrypt *all other* encrypted VMs, except that of the `nexus` server [Nor20a]. However, the machine `inf-tang-app-01`, unlike the other key servers, required a password [Nor20a]. "With the EUROPOL technical assistance, this password 'theskeletonkey' was retrieved through the `inf-tang-app-01` machine, [[enabling]] the decryption of the volume of the `nexus` machine." [Nor20a]

The VMs were responsible for, among other things, managing cryptographic keys, event logs, customer support, notes and SIM cards [Lan21, ¶104].[34]

Business data. One server (`prd-oas-01`) contained a client management portal accessible via OpenVPN [Nor20a]. It held a "connection logging database, containing authentication logins, real IP addresses, and locations by country" of resellers [Nor20a]. Similarly, `prd-portal-live-app` and `prd-portal-live-db` "managed the customer management application" [Nor20a]. This provided data relating "to payments, users, resellers' pseudonyms linked to delivery addresses, the IMEI references of the phones, or the monthly data consumption of a SIM card in a country" [Nor20a]. This data was used to demonstrate Encrochat usage in France in warrant applications seeking authorisation for the later compromise [Nor20a].

EncroNotes. French law enforcement analysed a virtual machine responsible for managing EncroNotes [Lan21, ¶104], the user application for storing encrypted notes. The `prd-notepad-backup-app-01` machine was used for this purpose and other backups.[35] As mentioned above, EncroNotes were protected with a second password [Reg20]. Specifically, the notes were encrypted with SQLCipher[36] [Nor20a] whose key was encrypted with a password through the cacheword[37] library with a password entered by the user at the start of the application, at least 15 characters long [Nor20a]. Overall, 7,582 encrypted keys were identified and targeted for password cracking [Nor20a].[38] From

[33] `https://github.com/latchset/clevis`

[34] "machines handling encryption keys, analysis of the event logs, the application for user support, the SIM card usage feedback application, the virtual private network server for the initial configuration of the BQ devices (programming of the Encrochat system), the application for tracking SIMS assignments to devices and the corresponding database, the 'voice' call management application and the corresponding database, customer management application (resellers, stocks), the file exchange application." [Nor20a]

[35] "18,920 encrypted files in the 'contacts' directory, 35,955 encrypted files in the 'notepad' directory, 35,806 encrypted files in the 'roster' directory" [Nor20a]

[36] `https://www.zetetic.net/sqlcipher/`

[37] `https://guardianproject.info/code/cacheword/`

[38] "7,582 encrypted keys and encryption parameters were extracted to attempt to 'crack' passwords" [Nor20a]

those, for 981 passwords were identified by password cracking (so about 12.5%), which decrypted 8,725 files [Nor20a].[39] From this decrypted content, French investigators concluded these were used as ledgers in the drug trade [Lan21, ¶104], as emphasised in subsequent warrant applications.

TLS keys. As mentioned above, French law enforcement also recovered a TLS encryption key and shared it with the NCA in 2020.

5.3 Device compromise

30 January 2020. On 29 January 2020, the French prosecutor applied [Dec20e, Ber20a, Ber20c] for permission to break into Encrochat's servers to install, for one month, a "technical device whose purpose, without the consent of the persons concerned, is to access ... computer data, to record, store and transmit them, as they are stored in a computer system, as they are displayed on a screen for the user [[...]], as they are entered by character input or as they are received and transmitted by peripherals" [Nor20a]. This was granted on 30 January 2020 [Lan21, ¶115] for the period of one month. This warrant was granted for the 14 IP addresses and 3 IP /28 subnets mentioned in the application, all hosted by OVH SAS in Roubaix.[40] The prosecutor had applied to "set up a technical system" for:[41]

1. "access to the server on which all the data related to the functioning of the Encrochat system transit; this setup will be done on the premises of the company OVH located in Roubaix [[...]]" [Nor20c];[42]
2. "the installation of this technical system on the terminals that are connected to this server in order to function (i.e., Encrochat handsets), by means of a transmission over a [[...]] network" [Nor20c].[43]

That is, the request was for the permission to install malware on Encrochat phones ("terminals") and to install/modify servers in Encrochat's infrastructure to deploy and interact with this malware. However, only the latter action, interfering with the servers, was authorised at this stage [Nor20a].

3 February 2020. C3N solicits the support of STNCJ to implement the malware [Dec20f].

12 February 2020. On 11 February the French prosecutor reapplied with the additional request to capture data for devices communicating with any of these servers underlined in the application [Ber20d]. This was granted in full on 12 February [Lan21, ¶116] for one month [Lec20a].[44]

[39] "3462 given 'rooster' (contact lists), 1788 'contact' data (encrypted data, inaccessible without their decryption key), 3477 'notes' data (text files corresponding to notes or memos)" [Nor20a]

[40] The document [Nor20a] gives only 12 IP addresses, but this is a translation/transcription error since the French original gives 14 unique IP addresses (and three duplicates); [Lec20a] matches the French original on which [Nor20a] is apparently based.

[41] We cite the original French warrants here as these quotations are translations are our own. We found the English translation in [Nor20a] less clear, especially when excerpted.

[42] Original: "l'accès au serveur, sur lequel toutes les données visées de fonctionnement de la solution ENCROCHAT transitent; cette mise en place sera réalisée dans les locaux de la société OVH sise à ROUBAIX ... "

[43] Original: "la mise en place de ce dispositif au moyen d'une transmission par un réseau de communications électronique, sur les terminaux reliés, pour leur fonctionnement, à ce serveur"

[44] "AUTHORISE the installation for a period of one month of a technical device whose purpose, without the consent of the persons concerned, is to access ... computer data, to record, store and transmit them, as they are stored in a computer system, as they are displayed on a screen for the user [[]], as they are entered by character input or as they are received and transmitted by peripherals: [[...]] By means of transmission via an electronic communication network, on the terminals and peripherals connected for their operation to this server;" [Lec20a]

27 February 2020. The malware – "the technical solution for capturing data ('the implant')" [Eur20d] – was reported in a Europol meeting to work "in the lab but behaves differently when testing on the server" [Eur20d].

4 March 2020. On 3 March 2020 the prosecutor additionally applied [Dec20a, Ber20g] to block Gandi SAS and DNS Made Easy (both DNS providers) from interfering with the operation by making changes to the DNS configuration.[45] It also requested the authority to instruct OVH to implement a block preventing networking changes that affected the targeted virtual machines and IP addresses. This was to ensure the effectiveness of the authorised break-in and wiretap [Nor20b].[46] The DNS order related to `encrochat.ch` and all sub-domains. A list of 33 subdomains of `encrochat.ch` was provided in the warrant; see Table 7. This was granted on 4 March [Lan21, ¶117] for one month [Nor20b].[47] Also, the authorisations from the previous two warrants were renewed for one month.

At the time the warrant was applied for and approved, DNS Made Easy was the DNS provider of `encrochat.ch` according to historical name server and WHOIS records; see Tables 3 to 5. Gandi was the registrar until 4 April 2020 according to Switch [SWI24]. According to DomainTools [Dom24], no registrar is given since February 2019. Moreover, Certificate Transparency logs contain certificates for the domains `(www.)sims.encrochat.ch` issued by "Gandi Standard SSL CA 2" on 19 December 2020 and valid until 19 December 2021.[48] Overall, this suggests `encrochat.ch` was registered with Gandi SAS (the registrar)[49] but DNS services were provided by DNS Made Easy. This interpretation is confirmed in a letter by the police officer heading the Encrochat investigation dated 11 May 2021 and responding to a judge's request: "Note that the blocking of DNS resolution could be carried out at two levels, either through Gandi, the registrar for the encrochat.ch domain, or through the company DNS MADE EASY to which a DNS delegation was established." [Dec21b]

5 March 2020. By this date a meeting between French law enforcement and OVH took place and the process of copying the Encrochat "infrastructure" to C3N servers started [Eur20a]. We interpret this to mean that (parts of) the Encrochat server infrastructure were replicated by C3N based on the following sentence in the same document: "The control of [[the French authorities' server]] should be given to the French authorities during the weekend and a testing phase will start at the beginning of next week." [Eur20a] This is also supported in other documents [Eur20b, Eur20c] (see below for more discussion).

[45] The court order required "domain name registrar Gandi SAS and hosting company DNS Made Easy not to take any action that could impact EncroChat's Swiss-registered internet domains" [Goo21]. The measure was justified by the lead investigator as follows: "Given the complexity of the network comprising virtual machines, terminals, and connections via a domain, it was necessary to implement technical measures ensuring that interception efforts were not neutralised by configuration changes. Blocking any DNS modifications with Gandi was integral to preparing the digital data capture operation, serving as a safeguard against countermeasures from Encrochat administrators. [[...]] This seizure consequently led to the blocking of the domain name and its subdomains. This prevented any transfer of the domain name from Gandi to another registrar, notably foreign, which would have allowed Encrochat administrators to modify the DNS resolution associated with the domain name. In this scenario, data capture would have immediately ceased." [Dec21b]

[46] In [Goo21], this is expressed as the Lille court ordering the OVH data centre provider "not to take any action that would impact the network infrastructure, virtual machines and IP addresses associated with EncroChat, during the hacking operation".

[47] "AUTHORISE to ensure the effectiveness of our authorisation and for the same duration of one month – the blocking of any operation affecting the domain name Encrochat.ch and all the related sub-domains by the service provider Gandhi [[sic]] SAS; – the blocking by the DNS Made Easy service provider of all operations relating to the DNS resolution for the Encrochat.ch domain and in particular the sub-domains listed below, as well as all sub-domains associated with the Encrochat.ch domain; [[...]] – the blocking by the provider OVH of any operation affecting the network infrastructure associated with the Encrochat.ch domain, the sub-domains relating to virtual machines and IP addresses as shown in the present requests and authorisations;" [Nor20b]

[48] See `https://crt.sh/?q=encrochat.ch`, last accessed 24 November 2023.

[49] "a domain name Encrochat.ch, registered with the company Gandhi [[sic]] SAS" [Mor20a]

20 March 2020. On 18 March the prosecutor [Ber20f] additionally applied for permission to compel Gandi SAS to "redirect directly" the traffic for the domain `encrochat.ch` and its subdomains [Lan21, ¶118],[Bun22, ¶13],[Mor20a] to the OVH data centre.[50] This was authorised on 20 March for one month [Mor20a] and was again justified to prevent countermeasures.[51]

We interpret this to mean that Gandi SAS was ordered to provide DNS services for `encrochat.ch` directly, instead of these being provided by DNS Made Easy. This interpretation is confirmed by the previously cited letter by the C3N lead investigator: "Gandi, upon requisition, removed the DNS delegation with DNS MADE EASY so that DNS resolution would be carried out from its own DNS service. Gandi then blocked any modification of the DNS resolution." [Dec21b] The motivation apparently was that unlike DNS Made Easy, Gandi SAS is a French company, and thus directly within French courts' jurisdiction, as discussed in a WhatsApp chat between the lead investigator and an NCA officer.[52]

24 March 2020. The server infrastructure of the French police was reportedly ready and French and Dutch law enforcement officers were running tests [Eur20c]. Reportedly, 96 virtual machines needed to be installed in order to "replicate" the Encrochat infrastructure [Eur20b]. Records of a Europol meeting on this date note that "[[t]]he technical solution was also tested and it's working" [Eur20c]. Here, as before, 'technical solution' appears to refer to the malware.

29 March 2020. On 26 March 2020 and on 29 March 2020 new certificates were issued for the domain `*.encrochat.network` using a Cloudflare service instead of Let's Encrypt or Sectigo, which had been exclusively used until then for that domain [Sec23]. Similarly, querying historic DNS data, from 27 March to 31 March 2020 the domain `encrochat.network` pointed to a Cloudflare IP instead of a Namecheap IP address. That domain used Namecheap IPs, according to the historic DNS data available to us, exclusively from November 2018 to March 2020 and again from April 2020 to September 2021.[53] This might indicate someone enabling Cloudflare proxy services and may either be an artefact of the French law enforcement operation, an attempted countermeasure by the Encrochat administrators, or entirely unrelated. The domain `encrochat.network` is never mentioned in any of warrants we have access to, suggesting this is unrelated to the law enforcement operation.

30 March 2020. The malware, referred to as a "device", "implant" or "technical solution" and developed by the French intelligence unit STNCJ, was delivered to C3N. It had been requested on 3 February 2020. It was stored on an 8GB USB key and placed in a secure vault [Dec20d]. It is unclear how experiments could have been conducted with the malware as early as 27 February 2020 without it having been delivered to C3N until 30 March. A possible interpretation is that C3N were reporting on STNCJ's progress in testing the malware in [Eur20d].

[50] "AUTHORISE, for a period of one month, the setting up by Gandi SAS of a redirection of the traffic linking the Encrochat.ch domain name to all the sub-domains that are attached to it, and which are thus identified: [[...]] so that they can be redirected directly to the OVH provider." [Mor20a]

[51] "It therefore appears necessary, in order to effectively implement the capture solution authorised by the ordinances of 30 January 2020 and 12 February 2020, in addition to the blocking authorised by the supplementary ordinance of 4 March 2020, to ensure DNS redirection so that requests are directed to the servers supporting the Encrochat infrastructure, hosted by the OVH service provider. This operation is essential to avoid any manipulation or intervention of the site administrators on the domain names or sub-domains;" [Mor20a]

[52] "[18/03/2020, 18:07:27] Jeremy: We don't need [[redacted in source]]
[18/03/2020, 18:07:32] Jeremy: we have a solution
[18/03/2020, 18:07:50] Jeremy: with the registrar of the domain name
[18/03/2020, 18:08:14] Jeremy: it's a French comapny [[sic]] and with an court order [[redacted in source]]
[18/03/2020, 18:08:27] Emma: [[...]]
[18/03/2020, 18:09:01] Jeremy: they replaces the [[redacted in source]] bu [[sic]] their own service" [SD20].

[53] Queried using `https://completedns.com/dns-history/` on 23 November 2023.

30 March 2020. There was an outage at the OVH data centre in Roubaix due to a claimed "router malfunction" [Jud20]; it is unclear if this is related to law enforcement efforts. We note that on this date the law enforcement operation did not have permission to change OVH's internal routing tables, which was applied for and granted the next day [Har20a] (see below), but it had the authority to instruct OVH to implement a block preventing networking changes that affected Encrochat since 4 March 2020 [Nor20b]. Given the later hiccups in a similar step by Gandi and the proximity of this event to the beginning of the malware campaign, a possible interpretation is that something went wrong here, too.

31 March 2020. On 31 March, the prosecutor additionally applied [Ber20h] for permission to compel OVH to redirect traffic towards law enforcement's infrastructure, specifically on load balancers [Bun22, ¶16],[Lan21, ¶119].[54] This was granted on the same day, with the restriction that only the Encrochat update functionality should be affected [Bun22, ¶16],[Lan21, ¶119].[55] The rerouting was implemented for `update.encrochat.ch` from 1 April [Dec21b]. Also, the authorisation for the DNS redirect, initially granted on 20 March 2020, was extended for one month.[56]

1 April 2020. According to first-party WHOIS records [SWI24], on 1 April, the DNS nameserver for `encrochat.ch` changed from `dnsmadeeasy.com` to `gandi.net` at 12:01 (presumably Swiss time, which matches French time); see Table 2. The same data reports it reverted to `dnsmadeeasy.com` that day at 23:01. Third-party WHOIS data [Dom24] also shows this change, albeit with the latter change being recorded two days later; see Table 4. The name server history also available in [Dom24] similarly shows a change of DNS hosting provider between 2 April and 3 April, see Table 3. We speculate the delay is an artefact of how often these records are queried/updated by `domaintools.com`.

This change is consistent with the approval obtained on 20 March 2020. However, the short period of the change – only coinciding with the planting of the malware update but not with the remainder of the operation – does leave open the question of what role the redirect played. This question is resolved in a letter by the French lead investigator which discusses that Gandi made a mistake in implementing the court order.[57]

1 April 2020. On 1 April at 17:15 (French time), French law enforcement injected their malware into the update servers of Encrochat devices [Lan21, ¶120]. The operation took 5 minutes [Lan21, ¶120],[Dec20c, Ber20b].

[54] "It appears that the operation of accessing the Encrochat server at OVH to capture data on this infrastructure and the related terminals requires the service provider to modify the network routing rules in order to redirect the flow from a technical load balancing device called loadbalancer from the customer's infrastructure to that set up by the investigation department. [[. . .]] AUTHORIZE, for the purposes of carrying out the previously authorized digital data capture measure, the modification of network routing rules with the company OVH in order to redirect data flows from the Client Encrochat infrastructure to the data capture system set up by the national gendarmerie;" [Har20a]

[55] "RECALL that this operation should only generate a redirection of data flows during requests for updates from telephones that intervene in an automated manner at regular intervals; RECALL that communications should not be redirected as a result of this technical operation; they will continue to arrive on the Encrochat server and that there will be no redirection of communications between this server and the server set up by the national gendarmerie." [Har20a]

[56] "AUTHORISE, for a period of one month, the setting up by Gandi SAS of a redirection of the traffic linking the Encrochat.ch domain name to all the sub-domains that are attached to it, and which are thus identified." [Har20a]

[57] "On April 1, 2020, Gandi, upon requisition, removed the DNS delegation with DNS MADE EASY so that DNS resolution would be carried out from its own DNS service. Gandi then blocked any modification of the DNS resolution. This registrar made a technical error and did not set up the DNS resolution as requested. This mistake by Gandi caused an interruption in the Encrochat service. Consequently, we asked Gandi to restore the initial DNS configuration and unblock the encrochat.ch domain name. As such, the Encrochat service was functional again. The service disruption necessarily drew the attention of Encrochat administrators, so it was decided to maintain the initial configuration and consequently not attempt another block on both the domain name and DNS resolution. Indeed, administrators could have logged into their Gandi client interface and noticed the blocking measures. Our data capture operation would then have been revealed. [[. . .]] The DNS resolution blocking was implemented from 12:00 to 23:30 on April 1, 2020. It was lifted under the conditions described above." [Dec21b]

Table 2: WHOIS records for `encrochat.ch` in the period covering 1 January 2019 to 31 December 2020 [SWI24].

date & time	type	from	to
2020-07-07 15:47	ns	ns0.dnsmadeeasy.com ns1.dnsmadeeasy.com ns2.dnsmadeeasy.com ns3.dnsmadeeasy.com ns4.dnsmadeeasy.com	–
2020-04-04 19:42	reg	Gandi	Hostpoint
2020-04-01 23:11	ns	ns5.dnsmadeeasy.com ns6.dnsmadeeasy.com ns7.dnsmadeeasy.com	ns0.dnsmadeeasy.com ns1.dnsmadeeasy.com ns2.dnsmadeeasy.com ns3.dnsmadeeasy.com ns4.dnsmadeeasy.com
2020-04-01 23:01	ns	ns-134-c.gandi.net ns-155-a.gandi.net ns-99-b.gandi.net	ns5.dnsmadeeasy.com ns6.dnsmadeeasy.com ns7.dnsmadeeasy.com
2020-04-01 12:01	ns	ns0.dnsmadeeasy.com ns1.dnsmadeeasy.com ns2.dnsmadeeasy.com ns3.dnsmadeeasy.com ns4.dnsmadeeasy.com	ns-134-c.gandi.net ns-155-a.gandi.net ns-99-b.gandi.net
2019-11-09 14:26	Restore Domain by Registrar (Gandi)		
2019-11-09 14:26	Delete Domain by Registrar (Gandi)		

In the table above "reg" means a registrar change, "ns" means a nameserver change.

French law enforcement exploited an unspecified vulnerability [Liv21, ¶19] and according to an NCA witness quoted in [Liv21, ¶19], this vulnerability could "be patched at any time". A similar statement is made in a chat message from the French lead investigator to an NCA officer: "[21/03/2020, 12:42:29] Jeremy: We are in a difficult situation. We have to start as soon as possible because of the risk that administrators patch the system fail that we will use." [SD20] We are not aware of any document specifying whether this "system fail" or vulnerability was in the Encrochat servers or in the phones. Previously, the NCA witness just mentioned had speculated about a "CVE[58] based exploit".[59]

C3N planted malware targeting all BQ X2 Encrochat devices[60] through the official Encrochat

[58] `https://www.cve.org`

[59] "It looks like the French are planning to utilise their access to the EncroChat servers. Suspect it is a CVE based exploit for deploying on devices via the update server. Allows them to use intercept on the server to decrypt any data that passes through it . . . though not sure. Meanwhile, we may re-design the implant to make it less persistent. This involves removing the real-time exfil component instead focusing on a single hit DB exfil. An OP against an EncroChat device would look a little something like this: Hook device up on X3 during update; Deploy implant; Wait for app restart to trigger implant; Implant grabs DB, Key and exfil's it via current UDP system; Implant tides up; Implant removes itself. This way we can exploit a device and leave it in a relatively 'clean' state so we don't interfere with any implant deployed by the French." [Inv23, ¶29] Note that X3 here does not refer to the BQ X3 devices mentioned below as clarified by the author during interrogation in court.

[60] "on 1/4/2020 a data capture was set up on Encrochat telephones (Model BQ X2)" [Ale20c]

update channels.[61] The specifics of the malware are considered national secrets by the French state [Liv21, ¶28] (see §7). We discuss what we know about the malware in §5.4.

It had been remarked in Europol meetings where the attack was discussed that the malware would not and did not work on BQ X3 devices that were starting to appear for Encrochat: "A new phone is being sold BQ Aquaris X3. It has new operating system with different security levels therefore the technical solution implemented by the French colleagues will not work with these phones so no data will be generated." [Eur20c, Update from Netherlands].

4 April 2020. Encrochat administators migrated the Encrochat domain to a Swiss registrar (Hostpoint AG); see Table 2. Since only the domain name had been moved while continuing to point to the same OVH infrastructure, the law enforcement operation remained unaffected [Dec21b].

8 April 2020. During the night of 8 April to 9 April 2020, the Encrochat administrators modified the DNS resolution for the subdomain `update.encrochat.ch`. This prevented the malware being sent to new phones thereafter. However, phones that had previously received the malware continued to transmit their data to law enforcement [Dec21b]. Given that this measure seemingly locked out the attackers from at least deploying malware on new devices, the vulnerability discussed under 1 April might have been "patched" this way.

24 April 2020. A British police employee, namely an intelligence analyst, tipped off an Encrochat user about the law-enforcement operation against Encrochat users, including that law enforcement agencies were able to access encrypted data from the Encrochat service [Cro23]. This user then relayed that information to another Encrochat user: "I no [[sic]] a lady who works for the police. This is not hearsay. Direct to me. They can access Encro software. And are using to intercept forearms [[sic]] only at the moment. There [[sic]] software runs 48 hours behind real time. So have ur burns one day max. And try to avoid giving postcodes over it." [Nat23].[62]

Table 3: "Name Server History" for `encrochat.ch` [Dom24]

event date	action	previous server	new server
2023-09-10	delete	gandi.net	*none*
2022-09-02	new	*none*	gandi.net
2020-07-09	delete	dnsmadeeasy.com	*none*
2020-04-03	transfer	gandi.net	dnsmadeeasy.com
2020-04-02	transfer	dnsmadeeasy.com	gandi.net
2015-04-24	transfer	easydns.com	dnsmadeeasy.com
2013-11-08	transfer	gandi.net	easydns.com
2013-10-14	new	*none*	gandi.net

29 April 2020. The prosecutor applied for [Dec20b, Ber20e] and was granted an extension of one month [Mor20b],[Bun22, ¶17],[Lan21, ¶121].

? May 2020. Some Encrochat users reported that the remote wipe functionality was not working [Cox20a, Cox20b].

[61] " 'An implant within an Application will be placed on all Encrochat devices worldwide. This will be placed on devices via an update from the update server in France' " [Liv21, ¶25]

[62] For completeness we mention that we doubt that this strategy would have worked.

Table 4: WHOIS records for `encrochat.ch` [Dom24]

date	registrar	namerserver domain	extra
2022-08-31	*none given*	gandi.net	
2020-04-03	*none given*	dnsmadeeasy.com	
2020-04-01	*none given*	gandi.net	
2020-03-22	*none given*	dnsmadeeasy.com	+
2020-01-10	*none given*	dnsmadeeasy.com	
2019-03-29	*none given*	dnsmadeeasy.com	
2019-02-14	Gandi SAS	dnsmadeeasy.com	
2018-12-19	Gandi SAS	dnsmadeeasy.com	
2017-12-13	Gandi SAS	dnsmadeeasy.com	
2016-10-18	Gandi SAS	dnsmadeeasy.com	
2015-07-04	Gandi SAS	dnsmadeeasy.com	
2015-04-06	Gandi SAS	easydns.com	
2013-12-19	Gandi SAS	easydns.com	
2013-10-15	Gandi SAS	gandi.net	

Entries marked with "+" are taken from Whois records separately downloaded from `domaintools.com` but not included in [Dom24].

26 May 2020. By this date the malware had been installed on at least 20,000 Encrochat devices; more than 100K messages and 1,136GB of data had been captured [Bun22, ¶18],[Lan21, ¶122],[Ale20c].[63] As noted above, based on [Dec21b] all infections happened between 1 and 8 April.

28 May 2020. The prosecutor applied for and was granted a four-month extension [Ale20c],[Bun22, ¶20],[Lan21, ¶122].

9 June 2020. C3N noticed that test Encrochat phones were querying the update server via a new subdomain: `update.zerolegacy.ch` [Dec21b].[64] C3N had previously noted a new domain being used, presumably `zerolegacy.ch`, but for new phones only, presumably BQ X3.[65] Based on this fact and the entry for 10 June 2020 we interpret this to mean that what was new here is that also BQ X2 phones were contacting `zerolegacy.ch`.

10 June 2020. On 10 June, the public prosecutor applied for permission to extend the attack also to the subdomain `update.zerolegacy.ch` [Ale20a]. The approval specifically states that Encrochat devices – explicitly referred to as BQ X2 and BQ X3 devices, whereas earlier warrants only mention BQ X2 devices – queried `update.zerolegacy.ch` but chatted via `connect.encrochat.ch`.[66]

[63] "as on the 1/5/2020, approximately 28,000 telephones were sending data to the investigation service's storage server, that on the 26/5/2020 this figure concerned 20,429 telephones, that relay activations were recorded in 122 countries, that 100,800,000 messages were captured, and that 1,136 gigabytes (GB) of data were captured and stored;" [Ale20c]

[64] `zerolegacy.ch` does not appear in any earlier-dated documents we have seen.

[65] "[18/03/2020, 17:58:21] Jeremy: New phones are used by E company
[18/03/2020, 18:00:17] Jeremy: the update server for these new phone is associated to a new domain name. So we were afraid this morning because we thought that the server was migrating
[18/03/2020, 18:00:23] Jeremy: but It's not really like this...
[18/03/2020, 18:03:08] Jeremy: I'm not a technician I don't want enter to technical details but I can say, we have to start our operation soon but not tomorrow. Today, I was very busy. I think I'm still in the office for a long time... I didn't take a time for discuss all detail with our Dutch partners." [SD20]

[66] "That the connection tests carried out from the models BQ X3 and BQ X2 in order to identify the DNS requests sent by the terminals revealed a DNS request `update.zerolegacy.ch` for the two models BQ X3 and BQ X2; that

We give the hosting history of the domain `zerolegacy.ch` in Table 6 and first-party WHOIS history data in Table 5. The switch to Cloudflare in April, shown in Table 6, can be attributed to the Encrochat developers, as discussed in [Ale20a]. Table 7 provides a list of the subdomains we were able to identify.

Table 5: WHOIS records for `zerolegacy.ch` in the period covering 1 January 2019 to 31 December 2020 [SWI24].

date & time	type	from	to
2020-06-12 15:16	ns	daniella.ns.cloudflare.com elias.ns.cloudflare.com	ns-21-b.gandi.net ns-62-a.gandi.net ns-71-c.gandi.net
2020-06-12 15:10	ns	ns-21-b.gandi.net ns-62-a.gandi.net ns-71-c.gandi.net	daniella.ns.cloudflare.com elias.ns.cloudflare.com
2020-06-12 14:58	ns	daniella.ns.cloudflare.com elias.ns.cloudflare.com	ns-21-b.gandi.net ns-62-a.gandi.net ns-71-c.gandi.net
2020-04-17 21:50	ns	ns-1533.awsdns-63.org ns-1879.awsdns-42.co.uk ns-212.awsdns-26.com ns-687.awsdns-21.net	daniella.ns.cloudflare.com elias.ns.cloudflare.com
2020-02-15 01:40	ns	ns-21-b.gandi.net ns-62-a.gandi.net ns-71-c.gandi.net	ns-1533.awsdns-63.org ns-1879.awsdns-42.co.uk ns-212.awsdns-26.com ns-687.awsdns-21.net
2020-02-12 20:11	Domain Insert by Gandi		ns-21-b.gandi.net ns-62-a.gandi.net ns-71-c.gandi.net

In the table above "reg" means a registrar change, "ns" means a nameserver change.

? June 2020. Investigating the remote wiping bug reports from May, Encrochat found malware on an X2 device in June 2020 [Cox20a, Cox20b], which "was designed to conceal itself from detection, disable the phone's factory reset, record the screen lock password, and clone application data" [Cox20a].

Encrochat – within 48 hours [Cox24] – pushed an update to the X2 models "to restore the phone's features and gather information about the malware installed on its device" [Cox20b]. Moreover, "Encrochat put monitoring in place to be able to keep an eye on their devices without having to physically have it in their hands" [Cox20b]. An Encrochat representative commented "This was done to prevent further damage while we informed affected users" [Cox20b]. Note that by 9 April,

the chat application allowed text messages, photos, etc., to be sent, resulting in the appearance of a DNS request `connect.encrochat.ch` for the two models; that the tests carried out from the Encrochat telephones BQ X3 and Q X2 allowed the investigative team to determine that the two models, BQ X2 and BQ X3 were making their update requests to the sub-domain `update.zerolegacy.ch` and their communications requests to the sub-domain `connect.encrochat.ch` ..." [Ale20b]. An alternate English translation of that same French warrant, available as [Ale20a], contains an error in the quoted portion: [Ale20a] mentions a lack of reliability, which does not appear in [Ale20b] or the French original [Ale20d].

Table 6: DNS provider history for `zerolegacy.ch`, provided by `domaintools.com`

event date	action	pre-action server	post-action server
2020-03-17	new	*none*	awsdns-63.org
2020-04-19	transfer	awsdns-63.org	cloudflare.com
2020-06-14	transfer	cloudflare.com	gandi.net
2021-02-22	delete	gandi.net	*none*
2022-02-08	new	*none*	azure-dns.com

about two months earlier, Encrochat had regained control of `update.encrochat.ch`. But almost immediately after the patch, an enhanced version of the malware reappeared on devices.[67]

12 June 2020. The police employee who had tipped off a contact about the Encrochat investigation was arrested together with that contact [Nat23, Cro23].

12 June 2020. C3N started [Dec21b] rerouting traffic for `update.zerolegacy.ch` at OVH to distribute their malware again and data collection began including the X3 devices.[68] On this date, Cloudflare was disabled for `zerolegacy.ch` at 14:58, re-enabled at 15:10 and disabled again at 15:16 (presumably Swiss time); see Table 5. It is unclear who caused this.

Recall that, according to [Dec21b], C3N had lost its ability to infect new X2 devices with malware from 9 April. It seems plausible that the 12 June attack targeted both X2 and X3 devices. We speculate the Encrochat administrators may have pushed a "clean" update via `update.encrochat.ch` redirecting X2 devices to `update.zerolegacy.ch`, a URL that seemed to have been set up for BQ X3 devices (see also 9–10 June 2020), before C3N then deployed malware via `update.zerolegacy.ch`. We recall from 1 April 2020 that the method of exploitation for the X3 ("carbon") devices was reportedly different than the one used for X2 devices.

? June 2020. "Going into full-on emergency mode, Encrochat sent a message to its users informing them of the ongoing attack" [Cox20b].[69] Encrochat also informed its SIM provider (KPN) of the attack which then, upon Encrochat's request, blocked connections to the attacker's servers [Cox20b]. "As well as sending the message to users, Encrochat contacted its SIM card provider, the Dutch telecom KPN. Encrochat explained that an attack was ongoing and asked KPN to block what Encrochat said were malicious servers. KPN obliged. But within 160 minutes, KPN suddenly lifted those restrictions, and the hackers were back in." [Cox24]

13 June 2020. The Encrochat administrators issued a warning to their users via a "bulletin message" and advised them to destroy their handsets. The message specifically discusses the compromise of "carbon units", i.e. BQ X3 devices. Recall that Encrochat had already informed (at least) some BQ X2 users about the malware targeting X2 devices, as reported in [Cox20b]. Data collection

[67] The new version of the malware could change the lock screen password rather than just record it [Cox20a, Cox20b]. We believe this dates these events as occurring in the lead up to the new malware campaign starting on 12 June.

[68] "We collected data from X3 model devices on 12/06/2020 [[dd/mm/yyyy]] when the French deployed onto the new model and subsequently caused the compromise. As a result we have only a very narrow snapshot of the X3 devices whereas the data on the X2s collected, built up incrementally over time to develop the intelligence picture." [NCA20a]

[69] It is not clear if this "message" is the same as the warning message discussed under 13 June 2020. But given that the events described seem to respond to the malware campaign started on 12 June, we believe these events likely occurred on 12 or 13 June.

continued in diminished form (not all users heeded the warning) until July 2020.[70] According to an expert report [Rah23], the warning reads:[71]

> "Important Security Notice
> Date Issued: 2020-06-12
> Date Viewed: 2020-06-13
>
> Today we had our domains seized illegally by government entities. They repurposed our domain to launch an attack to compromise carbon units.
>
> With control of our domain, they managed to launch a malware campaign against the carbon to weaken its security.
>
> Due to the level of sophistication of the attack and the malware code, we can no longer guarantee the security of your device. We took immediate action on our network by disabling connectivity to combat the attack.
>
> You are advised to power off and physically dispose of your device immediately. Period of compromise was about 30 minutes and the best we can ascertain was about 50% of the carbon devices in Europe (due to the Updater schedule)." [Ree22]

Another expert report [And22a] shows a picture with the message on an Encrochat device, given the time as 9:09 on 13 June 2020. This seems likely to be UK time, given that the author of [And22a] reported to a British court. This version is very similar, but appears to contain several typos, such as the use of "manager" instead of "managed" and "dispose your device" instead of "dispose of your device". This screenshot appears to be of a regular (Encrochat) chat where perhaps a user reproduced the official Encrochat message. A different screenshot of the same message with the same incorrect spelling is also given in [Goo24]. However, the screenshot does not visually match that given in [And22a]; it appears to be of a different app or at least different app theme.

Overall, this could suggest that Encrochat developers discovered the 12 June 2020 attack specifically, and that this prompted this message and their shutdown.

5.4 The malware

We provide an overview of the on-device malware used in the attack, including the attackers' initial infection vector, on-device alteration, network topology and data exfiltration staging.

5.4.1 Initial infection vector.

In order to install new system applications, the attackers must have had access to the platform signing keys or must have exploited some vulnerability (e.g. a local privilege escalation). In the former case, given that the updater required updates to come from a domain with a pinned certificate (see §4.2), it would have been necessary for the attackers to have controlled `update.encrochat.ch`, along with the previously used key for that domain.

We consider it likely that the attackers had sufficient access, through control over the VM infrastructure at OVH, to install malware without leveraging an exploit on-device; control over the update server and appropriate signing keys would have been sufficient (at least for the better documented attack on X2 devices).

[70] "Overnight from the 12 to 13 June 2020 it became clear that the administrators of the Encrochat system were alerted to the attack upon their systems by Operation Emma. They issued a warning to their users which appeared on all of the Encrochat handsets advising the owners to 'power off and physically dispose your device immediately'. [[...]] Data collection continued, albeit diminishing in volume as a result of less use of the Encrochat handsets. The French authorities planned to seize the servers on 2 July 2020, and the JIT notified the NCA that all collection of data from the implants in the handsets ended at 18:48 on 1 July 2020" [Liv21, ¶68].

[71] In [Rah23] a screenshot of the message is shown. In this screenshot the message is declared a "bulletin message" and matches the wording reproduced in the main text.

5.4.2 On-device actions [Rah23].

The attackers modified platform-signed apps described in §4.2 rather than deploying entirely new applications, and similarly re-used network infrastructure provided by Encrochat to exfiltrate data and control user devices. *Admin* was updated with unspecified changes related to device policies involving password and data retention. *Marvin*'s changes caused it to behave similarly to a common piece of malware, using the servers at `marvin.encrochat.com` as a command and control server and supporting arbitrary data exfiltration. A core piece of functionality appears to be location extraction; Marvin would automatically scan for, collect and upload local Wi-Fi SSIDs, covertly enabling Wi-Fi if disabled on-device. The infected devices' *Updater* used `update.zerolegacy.ch` – still routed to Encrochat's servers at OVH – replacing `update.encrochat.ch`.

5.4.3 Malware and data exfiltration staging.

The malware installed on handsets worked in two stages [Liv21, SC22]. Similar to the way in which the attackers repurposed the already-existing applications on device, all data exfiltration occurred via Encrochat's servers at OVH [And22a, Shr22, And22b, Rah23]. We describe the two stages below.

Stage 1 was activated when the malware was installed or shortly thereafter and covered historical data collection, transmitting all data stored on the device to the French authorities, including "identifiers (e.g. IMEI and usernames), stored chat messages and notes (list not exhaustive)" [Liv21]. The extracted data included "messages, phonebook, Wifi (SSID), passwords, [[and]] call log" [Liv21, ¶73]. Much of the data was stored on device using the Realm[72] database software.

Stage 2 was a *live* collection phase in which chat messages were forwarded immediately to a French police server in real time.[73] The malware reportedly sent a copy of the plaintext message to the authorities, reportedly circumventing any end-to-end encryption [Liv21, ¶25].[74] We note that expert witnesses do not agree on the mechanism of data exfiltration [And22b, SC22, Shr22]. The data extracted was the same as in Stage 1, along with phone network cell IDs [Liv21, ¶73].[75]

To support real-time response to criminal activity on Encrochat during Stage 2, the attackers instituted a "threat-to-life" monitoring system [SG21], which was used to scan incoming data for keywords that could flag possible upcoming violent events.[76] Such messages would then be

[72] `https://realm.io/`

[73] "With the exception of some anomalous results, it appears that, in the main, the messages were packaged and ready for sending from the device in less than two seconds and that the messages were then exfiltrated and sent to the C3N server and available for reading a 'matter of seconds' later" [Liv21, ¶82] We note that the expert conviction that exfiltration happened via Encrochat's servers emerged in a later trial.

[74] "In relation to the operation of the device and the implant Mr Campbell explains that after user A's Encrochat device has been infected with the implant her message to user B would be sent as previously to the encryption protocol within the Encrochat app on the phone upon pressing send on the device. A copy would be made to the Realm, encrypted as before infection. As the direct result of the infection, an additional copy would be sent to the C3N implant. This C3N copy would be sent by the phone to the C3N server, and the message would also be sent as before to the Encrochat server. These operations within the phone would be simultaneous or almost simultaneous. The message would arrive with B, and if his device has also been infected then another copy of A's message would be made after it has been received and decrypted by the Encrochat app and would be sent by the implant to the C3N server." [Liv21, ¶83]

[75] "IMEI number; user nickname Encrochat; text message (SMS type) exchanged by users; Media files (photos, video voice messages, text documents) exchanged or stored in secure phones; identification number of triggered cells (these are the telephone relays); screen unlocking password and notes application password; notes, rosters and contact" [Mor20b]

[76] "6. TTL tool: a. At this time there is no option to add additional languages to the tool. The tool supports the identification of TTL events in French, English and Dutch. b. For the other languages, the countries mentioned the possibility to use wordlists. France mentioned that they are working on this functionality for their application. Netherlands mentioned that their TTL tool also supports importing a wordlist (CSV) c. UK suggested that the group should exchange wordlists in different languages. The participants accepted the proposal. Concrete discussions on how to exchange these didn't take place." [Eur20d]

reviewed and escalated for a potential intervention. To minimise exposure, C3N alerted further agencies to potential victims without indicating the source, to avoid disclosing the compromise of Encrochat [Eur20d].

5.4.4 Many details remain unknown.

The exact methodology, timing and structure of data sent during Stage 2 is opaque. Whereas Stage 1 had clear sourcing from on-device SQL and Realm databases, Stage 2 data was only delivered to the defence in parsed cleartext [Shr21e]. Although we can surmise from [Rah23, And22b] and the real-time response system that some significant amount of data did quickly pass through Encrochat's servers, we do not know exactly how this was achieved. As discussed further in §7, this lack of transparency became a point of contention in the following prosecutions, for reasons related to both criminal procedure and forensic accuracy of the data retrieved.

It is also unknown what the differences were between the implants deployed to specific devices, in the two attack waves. While it is documented that the attack vector was different (see 1 April 2020 in §5.3), whether exfiltration differed, too, is not clear. There is some evidence that malware deployed in the second attack on 12 June 2020 differs in its architecture from the one used on 1 April against X2 devices. In particular, [And22b] reports the following behaviour of a compromised X3 device:

> "7. the X3 device showed no evidence of an implant but clear evidence of modification to the EncroChat app itself, in that message burn times were no longer respected, specifically for the 'destroy your phone' emergency message;
>
> [[. . .]]
>
> 19. First, the X3 device attempts to communicate about every five minutes with a hardcoded IP address (`147.135.143.19`) on port 443 (https). This IP address appears to be owned by OVH, and resolves to the following page, suggesting a missing server behind a load balancer:
>
> [[. . .]]
>
> 20. It appears to be a reasonable hypothesis that the load balancer installed by DGSI would forward such traffic to an exfiltration server, because of the lack of DNS, the OVH IP address, the regular connection intervals and the fact that it is entirely in parallel with the communications with the MQTT server used by EncroChat devices for regular messaging.
>
> 21. The device also occasionally attempts to connect to `update.zerolegacy.ch` which may have been the update server from which the attack was launched.
>
> 22. However, the behaviour of the X2 device is rather different. There is no attempt to connect to `147.135.143.19` or to any other network address using any other protocol other than MQTT.
>
> 23. Our X2 attempted to send a series of messages to the MQTT server immediately upon connecting. We noticed that the data stream started with a message to the user ID `info.internal@encrochat.com` containing an IMEI number –the serial number of a mobile phone – and a SIM ID – which identifies the subscriber. These were not transmitted to the MQTT server by the unmodified EncroChat app used in the experiments by Luke Shrimpton which we replicated. This implies that the app on the X2 was modified."

5.5 Interpretation

The initial step in the Encrochat hack was law enforcement gaining control over the Encrochat update server, by a legal process targeting the server provider. Based on the information available

to us and laid out above, it appears likely that law enforcement then found a software-update signing key on Encrochat's servers; however, we have found no concrete indication that this happened, nor even any clear confirmation that law enforcement *had* an update signing key. What we do have documented is that they pushed the malware to phones via the update mechanism (see 1 April 2020 in §5.3).

If such a key (and presumably, Encrochat application source code) had been found on the servers, law enforcement would have been able to straightforwardly push a malicious software update that exfiltrated plaintext data, without breaking any cryptography.

In particular, it appears to us that French law enforcement were able to find system APK signing keys on OVH servers which allowed them to deploy their malware to Encrochat devices. While, in principle, the Encrochat developers could have disabled cryptographic verification of APK updates, they would have had to go out of their way to modify the Android base they started from (see §2.1). Thus, assuming that the developers did not take such drastic and invasive steps to weaken the security of their devices, in our view, the most plausible way an attacker could have deployed malicious software updates is by having access to the appropriate signing key. While an exploit could have been an alternative attack vector,[77] in our view, circumstantial evidence suggests law enforcement likely obtained a signing key, at least for the X2s. Such a key would have no business being accessible in a (public-facing) data centre. The matter's seriousness is escalated by the fact that Android does not provide a mechanism to revoke such signing keys on compromise: no PKI is used for these keys. Thus, a compromise of these keys is irrecoverable. We emphasise that our hypothesis that law enforcement found an update signing key is speculative, based on circumstantial evidence. Conclusively confirming or rejecting this hypothesis is an open question. Also, establishing the differences and similarities of the X2 and X3 campaigns, remains open.

While we have exhausted what we can deduce based on available documentation, reverse engineering could offer substantial further insight. Although we have a strong impression from our sources that it is difficult to obtain a device or image, this would be fascinating future work.

6 Open problems in cryptography

While it appears that the downfall of Encrochat can at least also be attributed to poor information security and development practices by the Encrochat developers, the attack also highlights important open problems for the cryptography and information security community.

6.1 Subversion of cryptography

The attack on Encrochat represents a prime example of the subversion of a cryptographic system by a state adversary: the breach of Encrochat was reportedly accomplished by side-stepping rather than breaking the end-to-end encryption (see §5.4).

Such attacks are discussed in the cryptographic literature predominantly as algorithmic substitution attacks (ASAs) [BPR14, BJK15, BL17, FM18, CHY20, HS21, BWP+22]. The techniques discussed in the ASA literature, though, would have had no bearing on the Encrochat attack, since the attackers apparently bypassed the end-to-end encryption entirely.

Supply chain security is often discussed in the context of JavaScript-based cryptographic solutions, see e.g. [BHP23, MPA23]. But, more broadly, given that most cryptographic software is not distributed directly by its producers but through various application stores – Apple, Google Play, Microsoft, Debian & Red Hat repositories, etc. – investigating techniques that secure the thus produced binary artefacts against third-party tampering is a pressing concern.

[77] This has been a subject of public speculation; see, e.g. `https://x.com/upsidedowntimes/status/1931300593957794112`. We note that the discussion of a patchable vulnerability from 1 April 2020 does not clarify this question, as it is unclear if that vulnerability is a device vulnerability.

However, in the case of Encrochat, measures such as binary transparency and reproducible builds may not have been effective countermeasures given that the attackers seemed to have had full control over a development environment used by the Encrochat developers. On the other hand, such measures would have given the Encrochat developers an opportunity to check their own activities against these logs to notice discrepancies. That said, the Encrochat developers could also have prevented or significantly complicated the attack by not storing the signing key on the servers at OVH (if, as we hypothesise, they did so), not keeping their key servers unencrypted, not relying on weak credentials, and so on.

6.2 Covert adversaries

This work also speaks to the extensive line of work in (applied) cryptography designing and analysing already-existing secure messaging systems [CCD+20, ACJM20, AMPS22, AMP+25, ADJ25, JK25, CGWZ25]. In particular, this literature, too, is concerned with state-level adversaries. In the cryptographic literature, the adversary – $\mathcal{A}$ – is an algorithm that has polynomial computing resources, controls the network and can compromise parties participating in the protocol.

A distinction between $\mathcal{A}$ and the adversary considered here – French law enforcement – is that the former is an arbitrary malicious adversary whereas the latter intended to remain undetected for an extended period of time. Thus, the adversary considered in this work can be modelled as a *covert adversary* [AL07].[78]

Indeed, it is remarkable that, as formalised in [AL07], the adversary here considered it worthwhile risking getting caught under some conditions by implementing a threat-to-life system (cf. §5.4).[79] Similarly, in [Cox24] it is reported that arrests based on the Encrochat data were carried out before the shutdown.

In contrast to covert adversaries in the cryptographic literature, however, the adversary here aimed to be eventually detected.[80] In particular, the complete destruction of Encrochat was the eventual aim of the law enforcement operation, after a period of covert operation.

Moreover, as reported throughout above, in stark contrast to "$\mathcal{A}$" in the literature, the attackers did not realise their ambition to remain covert and the operation was discovered at various points

[78] We note that in [AL07] covert adversaries are speculatively assumed and formalised rather than established: "In this work, we introduce a new adversary model that lies between the semi-honest and malicious models. The motivation behind the definition is that in many real-world settings, parties are willing to actively cheat (and as such are not semi-honest), but only if they are not caught (and as such they are not arbitrarily malicious). This, *we believe*, is the case in many business, financial, political and diplomatic settings, where honest behavior cannot be assumed, but where the companies, institutions and individuals involved cannot afford the embarrassment, loss of reputation, and negative press associated with being caught cheating. It is also the case, unfortunately, in many social settings, e.g. elections for a president of the country-club. Finally, in remote game playing, players may also be willing to actively cheat, but would try to avoid being caught, or else they may be thrown out of the game. In all, *we believe* that this type of covert adversarial behavior accurately models many real-world situations" [AL07, emphasis added].

[79] Formally, the adversary here decided whether to get caught based on the inputs of the honest parties to the Encrochat protocol, i.e. the Encrochat users. Thus, a definition wishing to rule out such an adversary would have to follow the "explicit cheat formulation" in [AL07] rather than the "failed simulation formulation" of a covert adversary.

[80] "ES [a UK NCA officer] confirmed that it is unknown if the users or EncroChat themselves will see the exploitation. There is a risk that the deployment will be a one off because of that. Part of the workshop will be to assess whether or not the deployment will be detected. The French intention is to deploy for 2 months as their warrants are one month in duration, to be extended for one month and thereafter to 'kill' EncroChat by destroying their reputation. The French and the Dutch will go public to say they have brought the server down." [Liv21, §19] The motivation for going public is spelled out more in a British warrant application: "After which the JIT plans to conduct overt law enforcement activity to cause total disruption to the EncroChat service. This will include the seizure of the French based servers and a large scale media campaign. It has been acknowledged that the Administrators of the EncroChat service could have a contingency plan in place and be in a position to re-instate their servers in another country. However, the seizure of the servers by the French Gendarmerie will likely cause significant disruption to the service in any event. The media campaign is intended to discredit the brand entirely with the intention that all users will cease using their phones immediately. The media campaign will publicise that the EncroChat service has been infiltrated by law enforcement and will likely include any successful law enforcement activity that has occurred as a direct result of the exploitation." [NCA20b]

throughout its lifetime. The continuity of the operation then relied on the incorrect interpretation of the evidence by the Encrochat developers, based on the data available to them at the time.

Just like "$\mathcal{A}$" in the literature, French law enforcement relied on control over the network. Indeed, the adversary in this work eventually literally assumed the role of message distributor similar to how adversaries are routinely modelled in the cryptographic literature, where the challenger asks the adversary to distribute messages. However, in order to gain and exercise this control it had to rely on third parties. While the French authorities did have the authority to compel OVH and Gandi to perform certain steps, they did not execute these steps themselves. In particular, as reported above, Gandi made a mistake in complying with the court order which interrupted the operation of Encrochat and thus could have been detected by the Encrochat administrators. Thus, the particular "implementation" of the adversary threatened its goals.

Finally, an adversary that is an organisation rather than an algorithm is also an adversary composed of people who may or may not have goals that align with this adversary. In the case of Encrochat, as described in our timeline above, the UK's prosecutor celebrated the conviction of a former intelligence analyst working on the Encrochat investigation who had tipped off a contact about the operation [Cro23].

We think the Encrochat hack serves as encouragement to cryptographic research to reconsider and refine the notion of covert adversaries.

7 Legal context

Our focus is on systematically understanding the technical aspects of what happened in the Encrochat compromise, not to provide legal commentary or critique (which is a separate and growing literature, as noted in §2.2). None of the authors has legal expertise in any of the jurisdictions involved in the Encrochat cases.

But during our research, we have found that the legal systems and proceedings involved provide valuable context for what happened and how we know what we know. This section provides a discussion of legal context and legal issues that is far from exhaustive, highlighting aspects that we found particularly interesting or significant in the context of our broader technically focused work, and doubtless leaving some important issues out.

In particular, recall that the Encrochat operation was a coordinated effort across multiple jurisdictions: France and the Netherlands comprised the Joint Investigative Team that led the effort, Europol assisted on behalf of the European Union, and other European countries were kept at least partially informed [Liv21]. The subsequent prosecutions took place across many countries as well, as also discussed above. Our limited review of legal context and documents focused primarily on France, the UK, and to a lesser extent, Germany.[81] This scope limitation is related to language abilities within the research team, as well as limited capacity.

Criminal procedure *Criminal procedure* refers to "the rules governing the mechanisms under which crimes are investigated, prosecuted, adjudicated, and punished" and "includes the protection of accused persons' constitutional rights" within any given legal jurisdiction [Gar24]. This includes rules around when government surveillance may take place, what investigative techniques are permitted under what conditions, and when the results of investigations can be used as evidence in legal proceedings, such as in court. The rules of criminal procedure vary by jurisdiction, as illustrated by the discussion below.

[81] We do reference occasional documents from other countries as well, but these are incidental findings.

7.1 Extent of criminal use

Recall that Encrochat phones had often shown up linked with criminal arrests, largely related to drug trafficking.[82] This prior evidence was among the justifications given for authorising the data capture operation.

The warrants and court cases in multiple countries emphasised the prevalence of criminal activity on the Encrochat network, contending that "Encrochat devices are used exclusively by criminals" and "there is no evidence of Encrochat devices being used for legitimate communication purposes" [Liv21].[83] While Encrochat does seem to have been heavily used for organised crime, and the investigation resulted in evidence to support the idea that a significant fraction – perhaps a majority – of Encrochat devices were used for organised crime,[84] we have seen no evidence that (almost) all Encrochat devices were used for criminal activity. The UK operation examined about 300 devices (almost 4% of users) that did not contain evidence of criminality (some of which did not contain much data at all); despite this, the Government maintained their assessment that these were not legitimate users [NCA20a]. Such arguments contributed to the justification for compromising the whole network rather than, for example, targeting individual Encrochat users who were suspected of criminal activity.[85]

Such claims of exclusive criminality would be easily disproved by counterexample, with respect to many other private communication tools, such as WhatsApp, Signal, or Tor, and even other "crypto phones"[86]. But curiously, counterexamples have been elusive in the case of Encrochat.[87] The absence of counterexamples, in itself, is far from proving exclusive criminality, and legal commentators have raised concerns about the sufficiency (and secrecy) of the evidence of exclusive criminality to support the compromise of the entire network in the Encrochat operation (e.g., [The21, Sto23]). Defendants have challenged the sufficiency and secrecy of this evidence in court; a difficulty in these challenges is that all the relevant information is in the Government's control, and much of the underlying

[82]The criminal charges listed in the warrants authorising the operation related to drug trafficking and to violating restrictions on distributing cryptographic tools under French law [Nor20a]. The overwhelming majority of discussion in the warrants focuses on drug trafficking, not cryptography controls. It appears that the drug charges provide the real justification for this investigation, and would have been sufficient without the cryptography-related charges. The idea of law enforcement targeting individuals for the use or distribution of cryptography alone has been controversial and heavily criticised (e.g. [Kay15, Gra05, IF24]) – that said, the prosecutions based on Encrochat data are far from this type of scenario, given the extensive evidence of criminality unrelated to cryptography on which the legal proceedings are based. For further discussion on cryptography controls in France, we refer to [La].

[83]Legal documents in other jurisdictions make similar suggestions that Encrochat was exclusively criminal. For example, a French warrant refers to "the dedicated nature of this encrypted telephone solution for criminal purposes" [Mor20b]. A German case went even further, and suggested that "a criminal organization ... aimed at trafficking in or handling large quantities of narcotics, maintained a highly specialised communications system ... possibly under the guise of the 'public' and advertised Encrochat solution ... which ... was made accessible only to the members of the organization for the purpose of conducting its illegal and large-scale narcotics transactions ... " – that is, that only criminals could use Encrochat [Lan21, ¶358].

[84]"Of the 380 telephones active [in France], 242 telephones (63.7%) are used for illicit or criminal purposes..." [Mor20b].

[85]Prosecutors' justifications for the operation also included fallacious arguments that the use of cryptography or certain privacy features (such as disappearing messages) is adequate cause for suspicion in itself. For example, "The system provides a secure means for organised crime groups to communicate in relation to their criminal activity. The specific features of the Encrochat communication system, including the inbuilt facility to erase messages after a given period of time (seven days is the default setting), and the fact that Encrochat devices can only communicate with other Encrochat devices, reinforces the conclusion that has been reached in relation to their use by the criminal community." [Liv21]; "In addition, EncroChat and Sky ECC were commonly known for their distant panic and password wipe abilities; features that no chat application reasonably needs – unless its users have something to hide." [Sag23] Such fallacious arguments commonly appear in other contexts as well, in reference to privacy technologies such as encryption, Tor, or others that are well known to have a variety of uses, whose legality varies by jurisdiction (e.g. [Bar21, Sch14, Sch08]). See also [Sol07] for a broader discussion of this type of fallacy.

[86]Blackphone was sold to "special forces, corporates, high-net-worth individuals, and human-rights workers" [And22a].

[87]The only documented example we have come across involves the use of Encrochat by a defence lawyer, who was not a criminal, to communicate with his "gangster" clients, who were criminal defendants [Cox24].

evidence has not been disclosed because it is classified.

7.2 Use of the evidence in prosecutions

National defence secrets under French law.

Information about the "operation of the technical system of data capture" is classified as a national defence secret under French law[88] because the operation was carried out by the STNCJ, within the DGSI.

The court authorising the technical operation[89] has discretion to order the operation be undertaken by the DGSI, as in this case; once the DGSI is thus involved, the details of the operation are necessarily classified as national defence secrets.[90] Our understanding is that enlisting the DGSI to execute a data collection is fairly routine, and the DGSI's involvement does not necessarily indicate that an operation involves especially sophisticated techniques.

Moreover, it appears to be standard and established procedure under French law to keep national defence secrets even from the judge presiding over a technical operation and issuing the authorisation for its execution.[91] While the warrants issued at Lille contained fairly detailed information on certain aspects of the Encrochat operation, the judges involved would not have had access to the full details of how the operation worked, due to national defence secrecy.

The Encrochat cases raised arguments that the lack of information about how evidence was gathered infringed on constitutional rights to a defence and a fair trial – that defendants and their lawyers could not mount an effective defence when so much critical information was kept from them. A legal case raising these arguments, and arguing that numerous other fundamental rights were violated in the Encrochat cases, reached the highest constitutional authority in France (the *Conseil Constitutionnel*), which ruled in favour of the Government – that is, that the national defence secrecy in the Encrochat cases fully respected French constitutional rights.[92]

Using national defence secrets in French courts.

French law prescribes that information collected using procedures protected under national defence secrecy must be accompanied by a "certificate of authenticity"[93] when introduced in court proceedings. In 2022, the *Cour de Cassation*, which is France's highest court for civil and criminal cases, determined that this requirement was violated in at least one French Encrochat prosecution.[94] It remains to be seen what effects such violations may have on other cases in France and abroad.

"Interception" and "equipment interference" in UK courts.

UK law distinguishes between two types of techniques, "targeted interception" (TI) and "targeted equipment interference" (TEI), roughly depending on whether data was exfiltrated in transit or at rest [UK 23, dec21a]. Whether the malware in Encrochat conducted TI or TEI (or perhaps both)

[88] In French, *secrets de la défense nationale.* Art. 413-9, Code Pénal, available at `https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000020933029`.

[89] In our case, the Douai Appeal Court (*Cour d'Appel de Douai*) at the Lille Judicial Tribunal (*Tribunal Judiciaire de Lille*).

[90] Art. 706-102-1, Code de Procédure Pénale, available at `https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311624`.

[91] National defence secrets may only be communicated as described in Arts. L. 2312-4 to L.2312-8 of the Defence Code (*Code de la Défense*).

[92] Decision No. 2022-987 QPC of 8 April 2022, available at `https://www.conseil-constitutionnel.fr/decision/2022/2022987QPC.htm`.

[93] Art. 230-3, Code du Procédure Pénale, available at `https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032656013`.

[94] Cour de Cassation, Pourvoi n° 21-85.148, available at `https://www.courdecassation.fr/decision/634510f19aeccbadff064d4c`.

determines whether the data collected through it is admissible as evidence in UK courts [Liv21, Pum22, dec21a]. When this critical evidentiary question arose in UK courts, the British submitted a request to the French to clarify certain aspects of how the exfiltration worked, which would determine whether the technique was TI or TEI; the French refused to answer, citing national defence secrecy [Liv21].

The British prosecutions then proceeded without this information, with both sides calling expert witnesses to render their opinion on how the exfiltration was likely to have worked, based on the incomplete evidence available (including analysis of artifacts not available to the public) (e.g. [Liv21, Rah23, And22b, Int21]).[95]

From our perspective as researchers trying to understand how the operation worked, the distinction between TEI and TI led to detailed even if often uncertain or speculative discussion of certain aspects of how the malware worked, which might not otherwise have been much or at all discussed publicly. These discussions helped us to piece together the story as much as we have.

Cross-border transfer of evidence.

The French distributed considerable amounts of exfiltrated data to other countries throughout at least the live phase ("Stage 2"; see §5.4) of the operation. These countries agreed to certain terms including keeping the data and source confidential while the operation was ongoing, and generally received data corresponding to users physically located in their jurisdictions at the time of data exfiltration. German cases have had a notable focus on whether the correct procedures for cross-border transfer of evidence within the European Union were followed in Encrochat cases; some of these issues have reached the Court of Justice of the European Union.[96] In Dutch cases, the extent of involvement of the Dutch police, who were part of the Joint Investigative Team together with the French, is a potentially significant issue that could affect whether (some of) the evidence is treated as the result of a cross-border transfer from the French (governed by French criminal procedure) or as the result of a Dutch police investigation (governed by Dutch criminal procedure) [Oer23, TT25].

Fair trial and fundamental rights.

The secrecy surrounding the investigative techniques in the Encrochat operation has caused problems in the subsequent legal proceedings, and has made it harder if not impossible to present a thorough defence. Legal arguments that the Encrochat cases violated the right to a fair trial, the right to a defence and other fundamental and constitutional rights in France, the UK, Germany, and many other European countries have been raised in courts and in public discourse [Sto23, OvT22, vLBM$^+$22]. As mentioned above, in France the highest constitutional authority ruled in favour of the Government on this question.

Acknowledgements

We are grateful to (in alphabetical order) Joël Alwen, Domaintools, Duncan Campbell, Simone Colombo, Andrew Crocker, François Delerue, Rebecca Dent, Daniella Ferrari, Alexis Fitzjean Ó Cobhthaigh, Felix Freiling, Aude Géry, Bill Goodwin, Wendy Grossman, Alice Hutchings, Rikke

[95] One expert report [Rah23] (for the defence) notes that the expert received APKs extracted by the NCA "from allegedly infected and uninfected NCA test handsets," a TLS certificate for the Encrochat root CA, Encrochat devices of different models, and Encrochat server images dated 2019 – none of which are available to the public. But the expert report "emphasize[s] a key concern ... which is the lack of the evidence supporting the origin of this data as I am yet to be provided anything that demonstrates the actual method of capture, storage, and just as critical, the data processing techniques and measures taken to uphold the integrity of this data" and also emphasises that the server images provided were from *before* the hack.

[96] Case C-670/22, M.N. (EncroChat), available at `https://curia.europa.eu/juris/documents.jsf?num=C-670/22`.

Bjerg Jensen, Mattijs Jonker, Janet Kearney, Samantha Lim, Sylvain Métille, Steven Murdoch, Marilyne Ordekian, Elle Pearson, Kushvinder Raheloo, Lisa Rzepka, Peter Sommer, Thomas Souvignet, Mark Stephens CBE, Joe St Sauver, Switch.ch, Daniel Thomas, and to others who prefer to remain anonymous, for helpful discussions and assistance. D.S. was supported in part by Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery grant RGPIN-2022-03187.

References

[AAB+97] Hal Abelson, Ross Anderson, Steven M Bellovin, Josh Benaloh, Matt Blaze, Whitfeld Diffie, John Gilmore, Peter G Neumann, Ronald L Rivest, Jeffrey I Schiller, et al. The risks of key recovery, key escrow, and trusted third-party encryption. *World Wide Web Journal*, 2:241–257, 1997.

[AAB+15] Harold Abelson, Ross Anderson, Steven M Bellovin, Josh Benaloh, Matt Blaze, Whitfield "Whit" Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G Neumann, et al. Keys under doormats. *Communications of the ACM*, 58(10):24–26, 2015.

[ABD+15] David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelin, and Paul Zimmermann. Imperfect forward secrecy: How Diffie-Hellman fails in practice. In Indrajit Ray, Ninghui Li, and Christopher Kruegel, editors, *ACM CCS 2015*, pages 5–17. ACM Press, October 2015. doi:10.1145/2810103.2813707.

[ACJM20] Joël Alwen, Sandro Coretti, Daniel Jost, and Marta Mularczyk. Continuous group key agreement with active security. In Rafael Pass and Krzysztof Pietrzak, editors, *TCC 2020, Part II*, volume 12551 of *LNCS*, pages 261–290. Springer, Cham, November 2020. doi:10.1007/978-3-030-64378-2_10.

[ADJ25] Martin R. Albrecht, Benjamin Dowling, and Daniel Jones. Formal analysis of multi-device group messaging in WhatsApp. In Serge Fehr and Pierre-Alain Fouque, editors, *EUROCRYPT 2025, Part VIII*, volume 15608 of *LNCS*, pages 242–271. Springer, Cham, May 2025. doi:10.1007/978-3-031-91101-9_9.

[AL07] Yonatan Aumann and Yehuda Lindell. Security against covert adversaries: Efficient protocols for realistic adversaries. In Salil P. Vadhan, editor, *TCC 2007*, volume 4392 of *LNCS*, pages 137–156. Springer, Berlin, Heidelberg, February 2007. doi:10.1007/978-3-540-70936-7_8.

[Ale20a] Sophie Aleksic. Order Authorising the Use of a Data Capture Device (10 June 2020). https://www.documentcloud.org/documents/24479116-lille-warrants, June 2020. Translation of [Ale20d] by unknown authors used in UK courts. PERMALINK: https://web.archive.org/web/20250428033700/https://s3.documentcloud.org/documents/24479116/lille-warrants.pdf.

[Ale20b] Sophie Aleksic. Order Authorising the Use of a Data Capture Device (10 June 2020). Translation of [Ale20d] by unknown authors used in UK courts, June 2020.

[Ale20c] Sophie Aleksic. Order Authorising the Use of a Data Capture Device (28 May 2020). https://www.documentcloud.org/documents/24479116-lille-warrants, May 2020. Translation of [Ale20e] by unknown authors used in UK courts. PERMALINK: https://web.archive.org/web/20250428033700/https://s3.documentcloud.org/documents/24479116/lille-warrants.pdf.

[Ale20d] Sophie Aleksic. Ordonnance autorisant le recours à un dispositif de captation de données informatique (10 June 2020). No URL known, June 2020.

[Ale20e] Sophie Aleksic. Ordonnance autorisant le recours à un dispositif de captation de données informatique (28 May 2020). No URL known, May 2020.

[AMP+25] Martin R. Albrecht, Lenka Mareková, Kenneth G. Paterson, Eyal Ronen, and Igors Stepanovs. Analysis of the telegram key exchange. In Serge Fehr and Pierre-Alain Fouque, editors, *EUROCRYPT 2025, Part VIII*, volume 15608 of *LNCS*, pages 212–241. Springer, Cham, May 2025. doi:10.1007/978-3-031-91101-9_8.

[AMPS22] Martin R. Albrecht, Lenka Mareková, Kenneth G. Paterson, and Igors Stepanovs. Four attacks and a proof for Telegram. In *2022 IEEE Symposium on Security and Privacy*, pages 87–106. IEEE Computer Society Press, May 2022. doi:10.1109/SP46214.2022.9833666.

[Anda] System_app.te - Android Code Search. https://cs.android.com/android/platform/superproject/+/android-14.0.0_r51:system/sepolicy/private/system_app.te. PERMALINK: https://perma.cc/H56V-JV5B. URL: https://cs.android.com/android/platform/superproject/+/android-14.0.0_r51:system/sepolicy/private/system_app.te.

[Andb] Android Developers. Sign your app — Android Studio. https://developer.android.com/studio/publish/app-signing. PERMALINK: https://perma.cc/RKL2-QZ3H. URL: https://developer.android.com/studio/publish/app-signing.

[Andc] Android Open Source Project. Android Compatibility Definition Document. https://source.android.com/docs/compatibility/cdd. PERMALINK: https://perma.cc/R54H-HLEK. URL: https://source.android.com/docs/compatibility/cdd.

[And22a] Ross Anderson. Expert report of Professor Ross Anderson. No URL known, January 2022.

[And22b] Ross Anderson. Supplementary expert report of Professor Ross Anderson. No URL known, February 2022.

[Ave21] Derrick Avery. Operation Venetic Initial Examination and Analysis Report. No URL known, March 2021.

[Bar21] Asha Barbaschow. Acic believes there's no legitimate reason to use an encrypted communication platform. https://www.zdnet.com/article/acic-believes-theres-no-legitimate-reason-to-use-an-encrypted-communication-platform, May 2021. PERMALINK: https://web.archive.org/web/20250722044617/https://www.zdnet.com/article/acic-believes-theres-no-legitimate-reason-to-use-an-encrypted-communication-platform.

[Ber20a] Antoine Berthelot. Application for Authorisation of the Use of a Technical Tool for the Capture of Informatical Data. Translation of [Ber20c] by unknown authors used in UK courts, January 2020.

[Ber20b] Antoine Berthelot. Letter dated 2 April 2020. No URL known, April 2020.

[Ber20c] Antoine Berthelot. Requête complémentaire aux fins d'autorisation de recours à un dispositif de captation de données informatique. No URL known, January 2020.

[Ber20d] Antoine Berthelot. Requête Complementaire aux fins D'autorisation de Recours a un Dispositif de Captation de Donnees Informatiques. No URL known, February 2020.

[Ber20e] Antoine Berthelot. Requête Complementaire aux fins D'autorisation de Recours a un Dispositif de Captation de Donnees Informatiques. No URL known, April 2020.

[Ber20f] Antoine Berthelot. Requête Complementaire aux fins D'autorisation de Recours a un Dispositif de Captation de Donnees Informatiques (18 March). No URL known, March 2020.

[Ber20g] Antoine Berthelot. Requête Complementaire aux fins D'autorisation de Recours a un Dispositif de Captation de Donnees Informatiques (3 March). No URL known, March 2020.

[Ber20h] Antoine Berthelot. Requête Complementaire aux fins D'autorisation de Recours a un Dispositif de Captation de Donnees Informatiques (31 March). No URL known, March 2020.

[Ber20i] Antoine Berthelot. SUPPLEMENTARY REQUEST FOR AUTHORISATION TO USE A DEVICE TO CAPTURE COMPUTER DATABASE. No URL known, April 2020.

[Ber20j] Antoine Berthelot. SUPPLEMENTARY REQUEST FOR AUTHORISATION TO USE A DEVICE TO CAPTURE COMPUTER DATABASE (18 March). No URL known, March 2020.

[Ber20k] Antoine Berthelot. SUPPLEMENTARY REQUEST FOR AUTHORISATION TO USE A DEVICE TO CAPTURE COMPUTER DATABASE (3 March). No URL known, March 2020.

[Ber20l] Antoine Berthelot. SUPPLEMENTARY REQUEST FOR AUTHORISATION TO USE A DEVICE TO CAPTURE COMPUTER DATABASE (31 March). No URL known, March 2020.

[BGB04] Nikita Borisov, Ian Goldberg, and Eric A. Brewer. Off-the-record communication, or, why not to use PGP. In Vijay Atluri, Paul F. Syverson, and Sabrina De Capitani di Vimercati, editors, *Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society, WPES 2004, Washington, DC, USA, October 28, 2004*, pages 77–84. ACM, 2004. doi:10.1145/1029179.1029200.

[BHP23] Matilda Backendal, Miro Haller, and Kenneth G. Paterson. MEGA: Malleable encryption goes awry. In *2023 IEEE Symposium on Security and Privacy*, pages 146–163. IEEE Computer Society Press, May 2023. doi:10.1109/SP46215.2023.10179290.

[BJK15] Mihir Bellare, Joseph Jaeger, and Daniel Kane. Mass-surveillance without the state: Strongly undetectable algorithm-substitution attacks. In Indrajit Ray, Ninghui Li, and Christopher Kruegel, editors, *ACM CCS 2015*, pages 1431–1440. ACM Press, October 2015. doi:10.1145/2810103.2813681.

[BL17] Sebastian Berndt and Maciej Liskiewicz. Algorithm substitution attacks from a steganographic perspective. In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *ACM CCS 2017*, pages 1649–1660. ACM Press, October / November 2017. doi:10.1145/3133956.3133981.

[Bla94] Matt Blaze. Protocol failure in the escrowed encryption standard. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, and Ravi S. Sandhu, editors, *ACM CCS 94*, pages 59–67. ACM Press, November 1994. doi:10.1145/191177.191193.

[BPR14] Mihir Bellare, Kenneth G. Paterson, and Phillip Rogaway. Security of symmetric encryption against mass surveillance. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 1–19. Springer, Berlin, Heidelberg, August 2014. doi:10.1007/978-3-662-44371-2_1.

[BS20] Mihir Bellare and Igors Stepanovs. Security under message-derived keys: Signcryption in iMessage. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part III*, volume 12107 of *LNCS*, pages 507–537. Springer, Cham, May 2020. doi:10.1007/978-3-030-45727-3_17.

[Buc20] Ben Buchanan. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press, 2020.

[Bun22] 5 StR 457/21. Bundesgerichtshof, March 2022.

[BWP+22] Sebastian Berndt, Jan Wichelmann, Claudius Pott, Tim-Henrik Traving, and Thomas Eisenbarth. ASAP: Algorithm substitution attacks on cryptographic protocols. In Yuji Suga, Kouichi Sakurai, Xuhua Ding, and Kazue Sako, editors, *ASIACCS 22*, pages 712–726. ACM Press, May / June 2022. doi:10.1145/3488932.3517387.

[Cae20] Ed Caesar. The Cold War Bunker That Became Home to a Dark-Web Empire. The New Yorker. https://www.newyorker.com/magazine/2020/08/03/the-cold-war-bunker-that-became-home-to-a-dark-web-empire, August 2020. PERMALINK: http://archive.today/2021.11.29-094600/https://www.newyorker.com/magazine/2020/08/03/the-cold-war-bunker-that-became-home-to-a-dark-web-empire.

[Cae23] Ed Caesar. Crooks' mistaken bet on encrypted phones. The New Yorker. https://www.newyorker.com/magazine/2023/04/24/crooks-mistaken-bet-on-encrypted-phones, April 2023. PERMALINK: https://web.archive.org/web/20230424145529/https://www.newyorker.com/magazine/2023/04/24/crooks-mistaken-bet-on-encrypted-phones.

[Cam21] Duncan Campbell. What does the police hack of messaging service EncroChat mean for criminal prosecutions? https://www.youtube.com/watch?v=JogUfLFtVMU, March 2021.

[CCD+20] Katriel Cohn-Gordon, Cas Cremers, Benjamin Dowling, Luke Garratt, and Douglas Stebila. A formal security analysis of the Signal messaging protocol. *Journal of Cryptology*, 33(4):1914–1983, October 2020. doi:10.1007/s00145-020-09360-1.

[CGWZ25] Cas Cremers, Esra Günsay, Vera Wesselkamp, and Mang Zhao. ETK: External-operations TreeKEM and the security of MLS in RFC 9420. Cryptology ePrint Archive, Report 2025/229, 2025. URL: https://eprint.iacr.org/2025/229.

[Cha06] Kathy Charmaz. *Constructing grounded theory: A practical guide through qualitative analysis*. SAGE, 2006.

[CHY20] Rongmao Chen, Xinyi Huang, and Moti Yung. Subvert KEM to break DEM: Practical algorithm-substitution attacks on public-key encryption. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part II*, volume 12492 of *LNCS*, pages 98–128. Springer, Cham, December 2020. doi:10.1007/978-3-030-64834-3_4.

[CJZ11] Jon Callas, Alan Johnston, and Philip Zimmermann. ZRTP: Media Path Key Agreement for Unicast Secure RTP. RFC 6189, April 2011. URL: https://www.rfc-editor.org/info/rfc6189, doi:10.17487/RFC6189.

[CMG+16] Stephen Checkoway, Jacob Maskiewicz, Christina Garman, Joshua Fried, Shaanan Cohney, Matthew Green, Nadia Heninger, Ralf-Philipp Weinmann, Eric Rescorla, and Hovav Shacham. A systematic analysis of the juniper dual EC incident. In Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors, *ACM CCS 2016*, pages 468–479. ACM Press, October 2016. doi:10.1145/2976749.2978395.

[Cox20a] Joseph Cox. Encrypted Phone Network Says It's Shutting Down After Police Hack. Motherboard (Tech by Vice), June 2020. PERMALINK: https://web.archive.org/web/20221026085700/https://www.vice.com/en/article/5dz9qx/encrochat-hacked-shutting-down-encrypted-phone.

[Cox20b] Joseph Cox. How Police Secretly Took Over a Global Phone Network for Organized Crime. Motherboard (Tech by Vice), July 2020. PERMALINK: http://archive.today/2021.02.25-135931/https://www.vice.com/en/article/3aza95/how-police-took-over-encrochat-hacked.

[Cox21a] Joseph Cox. Emails Show Shadow Structure Behind Encrypted Phone Network Encrochat. Motherboard (Tech by Vice), March 2021. PERMALINK: https://web.archive.org/web/20231126135503/https://www.vice.com/en/article/4ad943/encrochat-owner-encrypted-phone-network.

[Cox21b] Joseph Cox. Encrypted Phone Firm Encrochat Used Signal Protocol. Motherboard (Tech by Vice), March 2021. PERMALINK: https://web.archive.org/web/20231018140359/https://www.vice.com/en/article/pkdjab/encrochat-signal-protocol-encryption.

[Cox24] Joseph Cox. *Dark wire*. PublicAffairs, New York, NY, June 2024.

[Cro23] Crown Prosecution Service. Ex-police employee caught leaking information about Operation Venetic is jailed. https://www.cps.gov.uk/cps/news/ex-police-employee-caught-leaking-information-about-operation-venetic-jailed, November 2023. PERMALINK: https://web.archive.org/web/20250503155327/https://www.cps.gov.uk/cps/news/ex-police-employee-caught-leaking-information-about-operation-venetic-jailed.

[dac20] Bureau des affaires criminelles. Retour sur l'affaire EncroChat, ou quand les cybergendarmes ont hacké la messagerie chiffrée utilisée par la criminalité organisée. https://www.gendarmerie.interieur.gouv.fr/gendinfo/criminalite-organisee-et-enquetes/2020/retour-sur-l-affaire-encrochat, July 2020. PERMALINK: https://web.archive.org/web/20250705135552/https://www.gendarmerie.interieur.gouv.fr/gendinfo/criminalite-organisee-et-enquetes/2020/retour-sur-l-affaire-encrochat.

[Das20] Jennifer Daskal. Transnational government hacking. *Journal of National Security Law and Policy*, 10, 2020.

[DC22] Max Daly and Joseph Cox. Cops Investigating 'WhatsApp for Gangsters' Arrest Key Suspect in Caribbean. Motherboard (Tech by Vice), June 2022. PERMALINK: https://web.archive.org/web/20231126135403/https://www.vice.com/en/article/jgpqv4/encrochat-arrest-paul-krusky.

[Dec20a] Jeremy Decou. Demande complémentaire dans le cadre d'une captation de données. No URL known, February 2020.

[Dec20b] Jeremy Decou. Demande de prolongation de captation. No URL known, April 2020.

[Dec20c] Jeremy Decou. Injection du dispositif de captation. No URL known, April 2020.

[Dec20d] Jeremy Decou. Letter dated 31 march 2020. No URL known, March 2020.

[Dec20e] Jeremy Decou. Request for authorisation to capture digital data. No URL known, January 2020.

[Dec20f] Jeremy Decou. Réquisition du service technique nationale des captations judiciaires. No URL known, February 2020.

[dec21a] decoded.legal. Encrochat, targeted equipment interference, and the court of appeal. https://decoded.legal/blog/2021/02/encrochat-targeted-equipment-interference-and-the-court-of-appeal, feb 2021. PERMALINK: https://web.archive.org/web/20250224235751/https://decoded.legal/blog/2021/02/encrochat-targeted-equipment-interference-and-the-court-of-appeal.

[Dec21b] Jeremy Decou. Letter dated 11 may 2021. No URL known, May 2021.

[dM20] Dick de Moor. Geheime chatdienst criminelen gekraakt: 'Grootste recherche-onderzoek ooit, een gamechanger'. RTV Utretcht, July 2020. PERMALINK: https://web.archive.org/web/20220217185058/https://www.rtvutrecht.nl/nieuws/2067014/geheime-chatdienst-criminelen-gekraakt-grootste-recherche-onderzoek-ooit-een-gamechanger.

[Dom24] Domaintools.com. Domain Report - Encrochat.ch. domaintools.com, January 2024.

[EE20] Europol and Eurojust. Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe. https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe, June 2020. PERMALINK: https://web.archive.org/web/20230429111141/https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe.

[Enc15] EncroChat. News. http://www.encrochat.network/news, 2015. PERMALINK: https://web.archive.org/web/20181022195934/http://encrochat.network:80/news.

[Enc19a] EncroChat. EncroChat Features. https://encrophone.com/en/, 2019. PERMALINK: https://web.archive.org/web/20190304151845/https://encrophone.com/en/.

[Enc19b] EncroChat. EncroChat Resellers. https://encrophone.com/en/resellers/, 2019. PERMALINK: https://web.archive.org/web/20190711113219/https://encrophone.com/en/resellers/.

[Enc19c] EncroChat. EncroChat Solutions. https://encrophone.com/en/solution/, 2019. PERMALINK: https://web.archive.org/web/20191008131820/https://encrophone.com/en/solution/.

[Esk20] Anthony Eskander. Protection from crime or covert erosion of rights. https://churchcourtchambers.co.uk/wp-content/uploads/2020/07/EncroChat-Article.pdf, July 2020. PERMALINK: https://web.archive.org/web/20230429105959/https://churchcourtchambers.co.uk/wp-content/uploads/2020/07/EncroChat-Article.pdf.

[Eur20a] Europol. Op. EMMA Conference call summary dated 05 March 2020. No URL known, March 2020.

[Eur20b] Europol. Op. EMMA Conference call summary dated 10 March 2020. No URL known, March 2020.

[Eur20c] Europol. Op. EMMA Conference call summary dated 24 March 2020. No URL known, March 2020.

[Eur20d] Europol. Op. EMMA Conference call summary dated 27 February 2020. No URL known, February 2020.

[Exp25] Involved Anonymous Technical Expert. Personal communication, June 2025. No URL known.

[Fae22] OPUS 2: Faetz and others v National Crime Agency, Day 1, September 2022. No URL known.

[FBI25] FBI.gov. Operation Trojan Shield, August 2025. https://www.fbi.gov/news/stories/fbi-global-partners-announce-results-of-operation-trojan-shield-060821. PERMALINK: https://web.archive.org/web/20260215043822/https://www.fbi.gov/news/stories/fbi-global-partners-announce-results-of-operation-trojan-shield-060821.

[FM18] Marc Fischlin and Sogol Mazaheri. Self-guarding cryptographic protocols against algorithm substitution attacks. In Steve Chong and Stephanie Delaune, editors, *CSF 2018 Computer Security Foundations Symposium*, pages 76–90. IEEE Computer Society Press, 2018. doi:10.1109/CSF.2018.00013.

[Gal20] Ryan Gallagher. European Police Hacked Secret Phone Network, Used AI for Major Bust. Bloomberg News, July 2020. PERMALINK: http://archive.today/2020.07.16-132616/https://www.bloomberg.com/news/articles/2020-07-16/european-police-hacked-secret-phone-network-used-ai-for-major-bust.

[Gar24] Bryan A. Garner. *Black's Law Dictionary*. Thomson Reuters, 12 edition, 2024.

[GGK+16] Christina Garman, Matthew Green, Gabriel Kaptchuk, Ian Miers, and Michael Rushanan. Dancing on the lip of the volcano: Chosen ciphertext attacks on apple iMessage. In Thorsten Holz and Stefan Savage, editors, *USENIX Security 2016*, pages 655–672. USENIX Association, August 2016. URL: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/garman.

[GJ24] Cerian Griffiths and Adam Jackson. Digital evidence, police investigations, and lessons learned from Encrochat: Is it time for a new framework for the admission of digital and communication evidence? *Criminal Law Review*, 2024.

[Goo18] Dan Goodin. Police decrypt 258,000 messages after breaking pricey IronChat crypto app . https://arstechnica.com/information-technology/2018/11/police-decrypt-258000-messages-after-breaking-pricey-ironchat-crypto-app/, November 2018. PERMALINK: https://web.archive.org/web/20250620191707/https://arstechnica.com/information-technology/2018/11/police-decrypt-258000-messages-after-breaking-pricey-ironchat-crypto-app/.

[Goo21] Bill Goodwin. Secrecy around EncroChat cryptophone hack breaches French constitution, court hears. Computer Weekly, June 2021. PERMALINK: https://web.archive.org/web/20231102173909/https://www.computerweekly.com/news/252501921/Secrecy-around-EncroChat-cryptophone-hack-breaches-French-constitution-court-hears.

[Goo22a] Bill Goodwin. NCA 'deliberately concealed' information when it applied for EncroChat warrants, tribunal hears. Computer Weekly, September 2022. PERMALINK: https://web.archive.org/web/20230429124300/https://www.computerweekly.com/news/252525205/NCA-deliberately-concealed-information-when-it-applied-for-EncroChat-warrants-tribunal-hears.

[Goo22b] Bill Goodwin. Police EncroChat cryptophone hacking implant did not work properly and frequently failed. Computer Weekly, March 2022. PERMALINK: https://web.archive.org/web/20231018142004/https://www.computerweekly.com/news/252514476/Police-EncroChat-cryptophone-hacking-implant-did-not-work-properly-and-frequently-failed.

[Goo23] Bill Goodwin. Three years on, EncroChat cryptophone hack nets 6,500 arrests and seizures of €900m. Computer Weekly, June 2023. PERMALINK: https://web.archive.org/web/20250619190334/https://www.computerweekly.com/news/366542786/Three-years-on-EncroChat-cryptophone-hack-nets-6500-arrests-and-seizures-of-900-million.

[Goo24] Bill Goodwin. WhatsApp and Signal messages at risk of surveillance following EncroChat ruling, court hears. Computer Weekly, July 2024. PERMALINK: https://web.archive.org/web/20250619190323/https://www.computerweekly.com/news/366596534/WhatsApp-and-Signal-messages-at-risk-of-surveillance-following-EncroChat-ruling-court-hears.

[Goo25] Bill Goodwin. Police swoop on Sky ECC cryptophone distributors in Spain and Holland. https://www.computerweekly.com/news/366618716/Police-swoop-on-Sky-ECC-cryptophone-distributors-in-Spain-and-Holland, January 2025. PERMALINK: https://web.archive.org/web/20250610101313/https://www.computerweekly.com/news/366618716/Police-swoop-on-Sky-ECC-cryptophone-distributors-in-Spain-and-Holland.

[Gra05] Jennifer Granick. Untitled. https://www.granick.com/archive/2005_05_01_theshout_archive.html#111758156022936540, May 2005. PERMALINK: https://web.archive.org/web/20221226173329/https://www.granick.com/archive/2005_05_01_theshout_archive.html#111758156022936540.

[Gre22] Geoff Green. I have been targeted by a malicious campaign of misinformation. https://medium.com/@Geoff_Green/i-have-been-targeted-by-a-malicious-campaign-of-misinformation-1c29e40142aa, January 2022. PERMALINK: https://web.archive.org/web/20231018133655/https://medium.com/@Geoff_Green/i-have-been-targeted-by-a-malicious-campaign-of-misinformation-1c29e40142aa.

[Har20a] Ali Haroune. Order Authorising the Use of a Data Capture Device (31 March 2020). https://www.documentcloud.org/documents/24479116-lille-warrants, March 2020. Translation of [Har20b] by unknown authors used in UK courts. PERMALINK: https://web.archive.org/web/20250428033700/https://s3.documentcloud.org/documents/24479116/lille-warrants.pdf.

[Har20b] Ali Haroune. Ordonnance autorisant le recours à un dispositif de captation de données informatique (31 March 2020). No URL known, March 2020.

[HS21] Philip Hodges and Douglas Stebila. Algorithm substitution attacks: State reset detection and asymmetric modifications. *IACR Trans. Symm. Cryptol.*, 2021(2):389–422, 2021. doi:10.46586/tosc.v2021.i2.389-422.

[Hut25] Alice Hutchings. Police behaving badly. *IEEE Secur. Priv.*, 23(1):80–82, 2025. doi:10.1109/MSEC.2024.3500152.

[HvW23] Pieter Hartel and Rolf van Wegberg. Analysing the impact of end-to-end encryption on the outcome of Dutch criminal court cases. *Crime Science*, 12, 2023.

[IF24] Mike Isaac and Sheera Frenkel. Telegram founder's indictment thrusts encryption into the spotlight. The New York Times, aug 2024. PERMALINK: https://web.archive.org/web/20250729155426/https://www.nytimes.com/2024/08/29/technology/telegram-encryption-pavel-durov.html.

[Int21] IntaForensics. AM/01 Technical Report. No URL known, 2021.

[Inv23] SF and Ors v NCA, 2023. https://investigatorypowerstribunal.org.uk/wp-content/uploads/2023/05/SF-and-Ors-v-NCA-JUDGMENT-IPT-21-05-CH-and-Ors-2023.pdf.

[Jak20a] Riaz Jakhura. Conference Operation Museful JIT required or not 8.1.20. No URL known, January 2020.

[Jak20b] Riaz Jakhura. Meeting Notes - Conference Operation Museful. Dated:- 03.02.2020. No URL known, February 2020.

[JG22] Adam Jackson and Cerian Griffiths. Intercepted communications as evidence: The admissibility of material obtained from the encrypted messaging service Encrochat. *The Journal of Criminal Law*, 2022.

[JK25] Joseph Jaeger and Akshaya Kumar. Analyzing group chat encryption in MLS, session, signal, and matrix. In Serge Fehr and Pierre-Alain Fouque, editors, *EUROCRYPT 2025, Part VIII*, volume 15608 of *LNCS*, pages 272–301. Springer, Cham, May 2025. doi:10.1007/978-3-031-91101-9_10.

[Jud20] Peter Judge. France's OVHcloud suffers brief outage. https://www.datacenterdynamics.com/en/news/frances-ovhcloud-suffers-brief-outage/, March 2020. PERMALINK: https://web.archive.org/web/20231018151452/https://www.datacenterdynamics.com/en/news/frances-ovhcloud-suffers-brief-outage/.

[Kay15] David Kaye. Report on encryption, anonymity, and the human rights framework. https://www.undocs.org/A/HRC/29/32, 2015. PERMALINK: https://perma.cc/QN7A-R9V5.

[La] La Quadrature du Net. Surveillance. https://www.laquadrature.net/surveillance. PERMALINK: https://web.archive.org/web/20250709131007/https://www.laquadrature.net/surveillance.

[Lan21] 46 KLs 3/21. Landgericht Hagen, June 2021.

[Lau20] Xavier Laurent. RE: 2020-03-02 Encrochat Server data European Investigation Order to France in English and French translation transmitted. No URL known, March 2020.

[Law20] Harewood Law. EncroChat: What you need to know. https://www.harewoodlaw.com/news/encrochat-what-you-need-to-know, July 2020. PERMALINK: https://web.archive.org/web/20230429120345/https://www.harewoodlaw.com/news/encrochat-what-you-need-to-know.

[Lec20a] Valerie Lecrohart. Order Authorising the Use of a Data Capture Device (12 February 2020). https://www.documentcloud.org/documents/24479116-lille-warrants, February 2020. Translation of [Lec20b] by unknown authors used in UK courts. PERMALINK: https://web.archive.org/web/20250428033700/https://s3.documentcloud.org/documents/24479116/lille-warrants.pdf.

[Lec20b] Valerie Lecrohart. Ordonnance autorisant le recours à un dispositif de captation de données informatique (12 February 2020). No URL known, February 2020.

[Liv21] R v Coggins, 2021. Liverpool Crown Court, Lexis Citation 291.

[May17] Jonathan Mayer. Government hacking. *Yale Law Journal*, 127, 2017.

[Mor20a] Hughes Mory. Order Authorising the Use of a Data Capture Device (20 March 2020). https://www.documentcloud.org/documents/24479116-lille-warrants, March 2020. Translation of [Mor20c] by unknown authors used in UK courts. PERMALINK: https://web.archive.org/web/20250428033700/https://s3.documentcloud.org/documents/24479116/lille-warrants.pdf.

[Mor20b] Hughes Mory. Order Authorising the Use of a Data Capture Device (29 April 2020). https://www.documentcloud.org/documents/24479116-lille-warrants, April 2020. Translation of [Mor20d] by unknown authors used in UK courts. PERMALINK: https://web.archive.org/web/20250428033700/https://s3.documentcloud.org/documents/24479116/lille-warrants.pdf.

[Mor20c] Hughes Mory. Ordonnance autorisant le recours à un dispositif de captation de données informatique (20 March 2020). No URL known, March 2020.

[Mor20d] Hughes Mory. Ordonnance autorisant le recours à un dispositif de captation de données informatique (29 April 2020). No URL known, April 2020.

[MPA23] Robertas Maleckas, Kenneth G. Paterson, and Martin R. Albrecht. Practically-exploitable vulnerabilities in the jitsi video conferencing system. Cryptology ePrint Archive, Report 2023/1118, 2023. URL: https://eprint.iacr.org/2023/1118.

[MSB+23] René Mayrhofer, Jeff Vander Stoep, Chad Brubaker, Dianne Hackborn, Bram Bonné, Güliz Seray Tuncay, Roger Piqueras Jover, and Michael Specter. The Android Platform Security Model (2023). Technical report, Google, 2023. URL: https://arxiv.org/pdf/1904.05572/1000.pdf.

[Nat20] National Crime Agency. NCA and police smash thousands of criminal conspiracies after infiltration of encrypted communication platform in UK's biggest ever law enforcement operation. https://www.nationalcrimeagency.gov.uk/news/operation-venetic, July 2020. PERMALINK: https://web.archive.org/web/20250612082249/https://www.nationalcrimeagency.gov.uk/news/operation-venetic.

[Nat23] National Crime Agency. Operation Venetic: Corrupt police worker jailed for tipping-off criminal over secret international investigation. https://www.nationalcrimeagency.gov.uk/news/operation-venetic-corrupt-police-worker-jailed-for-tipping-off-criminal-over-secret-international-investigation, November 2023. PERMALINK: https://perma.cc/ZXC2-T8DT.

[NCA20a] NCA. Operation VENETIC Briefing, dated 20 June 2020. No URL known, June 2020.

[NCA20b] NCA. TEI Authorites - Warrant No:- 91-TEI-0109-2020 - Op. Venetic. No URL known, March 2020.

[Nic16a] Ford Nickelson. Evidence suggests Encrochat is working with the NSA and other authorities. https://medium.com/@fordnic/evidence-suggests-encrochat-is-working-with-the-nsa-and-other-authorities-281bfd05ed9e, March 2016. PERMALINK: https://web.archive.org/web/20231018141605/https://medium.com/@fordnic/evidence-suggests-encrochat-is-working-with-the-nsa-and-other-authorities-281bfd05ed9e.

[Nic16b] Ford Nickelson. Weak PGP encryption and no security EncroChat. https://medium.com/@fordnic/weak-encryption-and-no-security-cbef2db2c300, March 2016. PERMALINK: https://web.archive.org/web/20231018143359/https://medium.com/@fordnic/weak-encryption-and-no-security-cbef2db2c300.

[Nor20a] Sandrine Normand. Order Authorising the Use of a Data Capture Device (30 January 2020). https://www.documentcloud.org/documents/24479116-lille-warrants, January 2020. Translation of [Nor20c] by unknown authors used in UK courts. PERMALINK: https://web.archive.org/web/20250428033700/https://s3.documentcloud.org/documents/24479116/lille-warrants.pdf.

[Nor20b] Sandrine Normand. Order Authorising the Use of a Data Capture Device (4 March 2020). https://www.documentcloud.org/documents/24479116-lille-warrants, March 2020. Translation of [Nor20d] by unknown authors used in UK courts. PERMALINK: https://web.archive.org/web/20250428033700/https://s3.documentcloud.org/documents/24479116/lille-warrants.pdf.

[Nor20c] Sandrine Normand. Ordonnance autorisant le recours à un dispositif de captation de données informatique (30 January 2020). No URL known, January 2020.

[Nor20d] Sandrine Normand. Ordonnance autorisant le recours à un dispositif de captation de données informatique (4 March 2020). No URL known, March 2020.

[Oer21] Jan-Jaap Oerlemans. Meer duidelijkheid over PGP Safe-operatie. https://jjoerlemans.com/2021/12/30/meer-duidelijkheid-over-pgp-safe-operatie/, December 2021. PERMALINK: https://web.archive.org/web/20250628110446/https://jjoerlemans.com/2021/12/30/meer-duidelijkheid-over-pgp-safe-operatie/.

[Oer23] Jan-Jaap Oerlemans. Meer duidelijkheid over EncroChat-operatie. https://jjoerlemans.com/2023/06/29/meer-duidelijkheid-over-encrochat-operatie, june 2023. PERMALINK: https://web.archive.org/web/20230630024040/https://jjoerlemans.com/2023/06/29/meer-duidelijkheid-over-encrochat-operatie.

[Oer24a] Jan-Jaap Oerlemans. Cryptocommunicatiedienst MATRIX ontmanteld. https://jjoerlemans.com/2024/12/12/cryptocommunicatiedienst-matrix-ontmanteld/, December 2024. PERMALINK: https://web.archive.org/web/20250628111319/https://jjoerlemans.com/2024/12/12/cryptocommunicatiedienst-matrix-ontmanteld.

[Oer24b] Jan-Jaap Oerlemans. Overzicht cryptophone-operaties. https://jjoerlemans.com/2024/12/13/overzicht-cryptophone-operaties, December 2024. PERMALINK: https://web.archive.org/web/20250628111608/https://jjoerlemans.com/2024/12/13/overzicht-cryptophone-operaties/.

[Oer25] Jan-Jaap Oerlemans. Meer duidelijkheid over de Exclu-operatie. https://jjoerlemans.com/2024/08/30/meer-duidelijkheid-over-de-exclu-operatie/, March 2025. PERMALINK: https://web.archive.org/web/20250628110410/https://jjoerlemans.com/2024/08/30/meer-duidelijkheid-over-de-exclu-operatie/.

[OR23] Jan-Jaap Oerlemans and Sofie Royer. The future of data-driven investigations in light of the Sky ECC operation. *New Journal of European Criminal Law*, 14, 2023.

[OvT22] J.J. Oerlemans and D.A.G. van Toor. Legal aspects of the Encrochat operation: A human rights perspective. *European Journal of Crime, Criminal Law and Criminal Justice*, 2022.

[PC17] R.L.D. Pool and B.H.M. Custers. The police hack back: Legitimacy, necessity and privacy implications of the next step in fighting cybercrime. *European Journal of Crime, Criminal Law and Criminal Justice*, 25, 2017.

[PC24a] Alexandra Posadzki and Joe Castaldo. Encrochat's Canadian leader knowingly sold encryption service to criminals, French authorities allege. `https://www.theglobeandmail.com/business/article-encrochats-canadian-leader-knowingly-sold-encryption-service-to/`, July 2024. PERMALINK: `https://web.archive.org/web/20250118122550/https://www.theglobeandmail.com/business/article-encrochats-canadian-leader-knowingly-sold-encryption-service-to/`.

[PC24b] Alexandra Posadzki and Joe Castaldo. France seeks extradition of another Canadian tied to Encrochat encrypted phone service. `https://www.theglobeandmail.com/business/article-encrochat-canadian-extradition-france/`, September 2024. PERMALINK: `https://web.archive.org/web/20250101153902/https://www.theglobeandmail.com/business/article-encrochat-canadian-extradition-france/`.

[Pfe24] Kristin Pfeffer, editor. *Policing Crime Chat Networks. Lessons from the Encrochat Operation*. Cuvillier Verlag, 2024.

[PS07] Vassilis Prevelakis and Diomidis Spinellis. The Athens affair. *IEEE Spectrum*, 44(7):26–33, 2007.

[Pum22] Pump Court Chambers. Decoding Encrochat: Admissibility. `https://www.pumpcourtchambers.com/2022/01/10/decoding-encrochat-admissibility`, January 2022. PERMALINK: `https://web.archive.org/web/20250428094033/https://www.pumpcourtchambers.com/2022/01/10/decoding-encrochat-admissibility`.

[Rah23] Kushvinder Raheloo. Expert report of Mr Kushvinder Raheloo, May 2023. No URL known.

[Ree22] Reeds Solicitors LLP. Encrochat Solicitors. `https://www.reeds.co.uk/encrochat-hack/`, 2022. PERMALINK: `https://web.archive.org/web/20230429105435/https://www.reeds.co.uk/encrochat-hack/`.

[Reg20] Matthieu Regnery. The dark phones (Encrochat) — criminals are building their own communication system. `https://xperylab.medium.com/the-dark-phones-encrochat-criminals-are-building-their-own-communication-system-474f3aeef759`, July 2020. PERMALINK: `http://web.archive.org/web/20230517134138/https://xperylab.medium.com/the-dark-phones-encrochat-criminals-are-building-their-own-communication-system-474f3aeef759`.

[Sag23] Georgios Sagittae. On the lawfulness of the EncroChat and Sky ECC-operations. *New Journal of European Criminal Law*, page 20322844231159576, 2023.

[SC22] Luke Shrimpton and Duncan Campbell. Joint Expert Report of Luke Shrimpton (...) and Dr Duncan Campbell. No URL known, February 2022.

[Sch08] Bruce Schneier. Using a file erasure tool considered suspicious. https://www.schneier.com/blog/archives/2008/07/using_a_file_er.html, July 2008. PERMALINK: https://web.archive.org/web/20230607132414/https://www.schneier.com/blog/archives/2008/07/using_a_file_er.html.

[Sch14] Bruce Schneier. NSA targets the privacy-conscious for surveillance. https://www.schneier.com/blog/archives/2014/07/nsa_targets_pri.html, July 2014. PERMALINK: https://web.archive.org/web/20250727094752/https://www.schneier.com/blog/archives/2014/07/nsa_targets_pri.html.

[SD20] Emma Sweeting and Jeremy Decou. WhatsApp Messages in English between 31/01/2020 and 06/04/2020. No URL known, 2020.

[Sec23] Sectigo Limited. Certificate transparency log for encrochat.network. https://crt.sh/?q=encrochat.network, 2023. PERMALINK: https://web.archive.org/web/20231102171344/https://crt.sh/?q=encrochat.network, last accessed 23 November 2023.

[SG21] Sebastian Klovig Skelton and Bill Goodwin. Dutch police used deep learning model to predict threats to life. Computer Weekly, May 2021. PERMALINK: http://web.archive.org/web/20230629102114/https://www.computerweekly.com/news/252500738/Dutch-police-used-deep-learning-model-to-predict-threats-to-life.

[Shr21a] Luke Shrimpton. Additional VENETIC Data Source Report #1. No URL known, May 2021.

[Shr21b] Luke Shrimpton. Additional VENETIC Data Source Report #2. No URL known, June 2021.

[Shr21c] Luke Shrimpton. EncroChat – Image Experiments. No URL known, November 2021.

[Shr21d] Luke Shrimpton. EncroChat – Message Status and Packet ID. No URL known, August 2021.

[Shr21e] Luke Shrimpton. VENETIC Data Source Report. No URL known, April 2021.

[Shr22] Luke Shrimpton. Expert Report – IPT. No URL known, February 2022.

[Ske24] Sebastian Klovig Skelton. Europol provides detail on Ghost encrypted comms platform takedown. https://www.computerweekly.com/news/366611232/Europol-provides-detail-on-Ghost-encrypted-comms-platform-takedown, September 2024. PERMALINK: https://web.archive.org/web/20250610102319/https://www.computerweekly.com/news/366611232/Europol-provides-detail-on-Ghost-encrypted-comms-platform-takedown.

[Sol07] Daniel J. Solove. 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review*, 44, 2007.

[Som21] Peter Sommer. Venetic/Encro: Understanding and Evaluating the Technical Evidence. https://www.25bedfordrow.com/cms/document/ps-encrochat-webinar-slides.pdf, March 2021. PERMALINK: https://web.archive.org/web/20230429111818/https://www.25bedfordrow.com/cms/document/ps-encrochat-webinar-slides.pdf.

[Sto23] Radina Stoykova. Encrochat: The hacker with a warrant and fair trials? *Forensic Science International: Digital Investigation*, 46:2666–2817, 2023.

[Swe20] Emma Sweeting. Eurojust Meeting Notes. No URL known, January 2020.

[SWI24] SWITCH Domain Info. [SWITCH#2024030210000794] Auskunftsgesuch encrochat.ch, zerolegacy.ch. private communication, March 2024.

[The21] Lukas Theune. Encrochat: – begründet allein der besitz eines sicheren telefons einen hinreichenden straftatverdacht, der den staatlichen hack erlaubt? *Kritische Justiz*, 54(4), 2021.

[TT25] Yelle Tieleman and Chiel Timmermans. Sprak Nederland de waarheid over de kraak bij Encrochat, ofwel 'de hack van de eeuw'? `https://www.ad.nl/binnenland/sprak-nederland-de-waarheid-over-de-kraak-bij-encrochat-ofwel-de-hack-van-de-eeuw~a582f724e/`, June 2025. PERMALINK: `http://archive.today/2025.06.17-005142/https://www.ad.nl/binnenland/sprak-nederland-de-waarheid-over-de-kraak-bij-encrochat-ofwel-de-hack-van-de-eeuw~a582f724e/`.

[UK 21] UK Cabinet Office. Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy. `https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy`, July 2021. Deep link: `https://assets.publishing.service.gov.uk/media/60644e4bd3bf7f0c91eababd/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf`; PERMALINK: `https://perma.cc/DC9U-8QHB`.

[UK 23] UK Home Office. Report on the operation of the Investigatory Powers Act 2016. `https://assets.publishing.service.gov.uk/media/63e22a4fd3bf7f1734709291/E02825581_Investigatory_Powers_Act_2016_ELAY.pdf`, February 2023. PERMALINK: `https://web.archive.org/web/20250623101849/https://assets.publishing.service.gov.uk/media/63e22a4fd3bf7f1734709291/E02825581_Investigatory_Powers_Act_2016_ELAY.pdf`.

[vLBM+22] J. van Laer, R. Binsard, G. Martine, A. Boret, C. Lödden, L.M. Barczyk, O. Wallasch, M. Rakow, D. Scheibner, J.C. Reisinger, R.D.A. van Boom, Y. Quint, R. Poppelaars, B. Janssen, M.O. Dietrichson, A. Krasniqi, J. Grahn, T. Schofield, I. Jinnah, O. Cook, S. Csoka QC, S. Choudhry, F. Hussain, and Fair Trials. Open letter of concern. `https://www.fairtrials.org/app/uploads/2022/02/EnroChat_LetterofConcern.pdf`, feb 2022. PERMALINK: `https://web.archive.org/web/20240723105827/https://www.fairtrials.org/app/uploads/2022/02/EnroChat_LetterofConcern.pdf`.

A Subdomains

We list known to us subdomains of `encrochat.ch` and `zerolegacy.ch` in Table 7.

Table 7: Encrochat.ch and zerolegacy.ch subdomains

[Nor20b, Mor20a, Har20a] encrochat.ch	enumeration encrochat.ch	enumeration zerolegacy.ch
		a1.
		a2.
		auth.a1.
	activate.	
bigend.		
billing.talk.	billing.talk.	billing.talk.
cerebro.	cerebro.	
chat.		
connect.	connect.	connect.
connect.talk.	connect.talk.	connect.talk.
currency.	currency.	currency.
demo.eportal.	demo.eportal.	
dmo.portal.	dmo.portal.	dmo.portal.
encrotalk.		
encrotalk2.		
encrotalk3.		
jasper.	jasper.	
marvin.	marvin.	marvin.
media.im.	media.im.	media.im.
my.		
mydevice.		
nexus.		
notes.	notes.	notes.
portal.		
proxy.talk.		
search.		
simple.	simple.	simple.
sims.	sims.	
stargate.	stargate.	stargate.
status.	status.	status.
test.		
update.	update.	update.
vanc.	vanc.	
	vpnas.	
www.cerebro.	www.cerebro.	
	www.demo.eportal.	
www.sims.	www.sims.	
x.		

We performed our enumeration with subfinder, where we enabled the `censys.io` data provider. We corrected typos in [Nor20b, Mor20a, Har20a] based on the French originals.

B Virtual machine and host names

The following list of 70 virtual machines is given in [Ave21, Appendix 1].

- centos_docker_template_02
- centos75-20180628-template
- dev-docker-test-box-01
- dev-themeapp-01
- inf-elasticsearch-01
- inf-foreman-app-01
- inf-idm-01
- inf-idm-02
- inf-nagios-app-01
- inf-pfsense-01
- inf-site24x7-puller-01
- inf-syslog-01
- inf-tang-01
- inf-tang-02
- inf-tang-app-01
- inf-tang-app-02
- New Virtual Machine
- pfSense-CE-2.4.3-RELEASE-amd64
- prd-activation-app-01
- prd-activation-db-01
- prd-billing-app-01
- prd-billing-app-02
- prd-bshd-app-01
- prd-bshd-app-02
- prd-bshd-db-01
- prd-bshd-gtw-01
- prd-bshd-redis-01
- prd-confluence-01
- prd-currency-01
- prd-devicesync-app-01
- prd-docker-crypto-template-01
- prd-immedia-app-01_1
- prd-immedia-app-02
- prd-jasper-01
- prd-jasper-app
- prd-jasper-app-02
- prd-marvin-app-01
- prd-marvin-db-01
- prd-nextcloud-01
- prd-nextcloud-db-01
- prd-notepad-backup-app-01
- prd-notepad-backup-clone
- prd-oas-01
- prd-osoz-app-01
- prd-portal-demo-app-01
- prd-portal-demo-db-01
- prd-portal-live-app-01
- prd-portal-live-db-01
- prd-portal-tunnel-01
- prd-push-01
- prd-simple-app-01
- prd-simple-db-01
- prd-status-app-01
- prd-status-app-02
- prd-themeapp-01
- prd-themeapp-db-01
- prd-updater-app-01
- prd-updater-app-02
- prd-updater-db-01

- prd-voip-call-app-01
- prd-voip-db-01
- prd-weblate-app-01
- stg-activation-app-01
- stg-activation-db-01
- stg-push-01
- stg-tunnel-01
- tst-bshd-01
- tst-crypto-migration-app-01
- tst-vm-01
- veeam_inf-pfsense-02-18-45-33-2018-09-25

The following list of 92 IP addresses and hostnames taken from "the hosts files found on 'inf-pfsense-01' " are given in [Ave21, Appendix 2]. Another source stated that 96 virtual machines needed to be installed in order to "replicate" the Encrochat infrastructure [Eur20b]

10.2.50.121 prd-immedia-app-01

10.2.50.122 prd-immedia-02

10.2.50.123 prd-bshd-app-01

10.2.50.124 prd-bshd-app-02

10.2.50.125 prd-bshd-redis-01

10.2.50.126 prd-bshd-db-01

10.2.50.127 prd-bshd-gtw-01

10.2.50.130 prd-currency-01

10.2.50.131 prd-jasper-app-01

10.2.50.132 prd-notepad-backup-app-01

10.2.50.133 prd-jasper-app-02

10.2.50.134 prd-jasper-db-01

10.2.50.135 prd-updater-app-01

10.2.50.136 prd-updater-app-02

10.2.50.137 prd-updater-db-01

10.2.50.140 dmo

10.2.50.140 prd-portal-demo-app-01

10.2.50.141 prd-activation-app-01

10.2.50.142 prd-activation-db-01

10.2.50.144 prd-portal-demo-db-01

10.2.50.145 prd-push-01

10.2.50.150 prd-themeapp-01

10.2.50.151 prd-themeapp-db-01

10.2.50.155 prd-voip-db-01

10.2.50.156 prd-status-app-01

10.2.50.157 prd-billing-app-01

10.2.50.158 prd-billing-app-02

10.2.50.159 prd-status-app-02

10.2.50.162 prd-simple-app-01

10.2.50.164 prd-simple-db-01

10.2.50.172 prd-portal-live-db-01

10.2.50.173 prd-devicesync-app-01

10.2.50.174 prd-portal-tunnel-01

10.2.50.175 prd-marvin-app-01

10.2.50.178 prd-marvin-db-01

10.2.50.180 prd-voip-call-app-01

10.2.50.190 prd-docker-crypto- template-01

10.2.50.22 prd-immedia-app-02

10.2.50.55 prd-osoz-app-01

10.2.1.115 inf-idm-01

10.2.1.116 inf-idm-02

10.2.1.120 inf-syslog-01

10.2.1.122 inf-elasticsearch-01

10.2.1.123 inf-tang-01

10.2.1.124 inf-tang-02

10.2.1.130 inf-foreman-app-01

10.2.1.130 prd-foreman-app-01

10.2.1.140 inf-site24x7-puller-01

10.2.1.4 inf-pfsense-carp

10.2.1.4 ns1

10.2.1.5 inf-pfsense-01

10.2.1.6 inf-pfsense-02

10.2.20.141 stg-activation-app-01

10.2.20.142 stg-activation-db-01

10.2.20.145 stg-push-01

10.2.20.174 stg-portal-tunnel-01

10.2.30.110 tst-bshd-01

10.2.40.130 dev-docker-test-box-01

10.2.51.11 prd-oas-01

10.2.51.170 eportal

10.2.51.170 prd-portal-live-app-01

10.2.51.99 tst-vm-01

10.2.55.110 prd-nextcloud-01

10.2.55.111 prd-nextcloud-db-01

10.2.55.115 prd-confluence-01

51.38.21.241 pfsense-wan-carp

51.38.21.242 pfsense-01-wan

51.38.21.243 pfsense-02-wan

51.38.21.244 billing-carp

51.38.21.245 marvin-carp

51.38.21.246 stargate-carp

51.38.21.247 portal-ovpnas-carp

51.38.21.248 connect-proxy-talk-carp

51.38.21.249 simple-carp

51.38.21.250 osoz-loader-carp

51.38.21.251 portal-dmo-carp

51.38.255.33 activation-carp

51.38.255.34 currency-carp

51.38.255.35 notes-carp

51.38.255.36 helpdesk-carp

51.38.255.37 imm-carp

51.38.255.38 themes-carp

51.38.255.39 jasper-carp

51.38.255.40 prd-push-01-wan

51.38.255.41 status-carp

51.38.255.42 prd-updater-app-01-wan

51.38.255.43 prd-updater-app-02-wan

149.56.251.50 Nexus

147.135.227.209 stg-push-01-wan

147.135.227.210 stg-activation-carp

192.168.70.15 inf-pfsense-01

192.168.70.15 lan-pfsense-01

C Extracted APKs

The lists of APKs in Tables 8 and 9 are reproduced from [Rah23].

Table 8: APKs extracted from an Encrochat BQ X2

Admin.apk	HTMLViewer.apk	SubstratumService.apk
AntHalService.apk	KeyChain.apk	SystemUl.apk
BlockedNumberProvider.apk	LatinIME.apk	TeleService.apk
CNEService.apk	Launcher3.apk	Telecom.apk
Calendar.apk	LegacyWipe.apk	TelephonyProvider.apk
CalendarProvider.apk	Marvin.apk	TimeService.apk
Capstone.apk	MediaProvider.apk	Updater.apk
CarrierConfig.apk	NvTerminal.apk	UserDictionaryProvider.apk
ConfURIDialer.apk	OfflineCalendar.apk	VpnDialogs.apk
Contacts.apk	OpenWnn.apk	WallpaperCropper.apk
ContactsProvider.apk	PacProcessor.apk	WallpaperPicker.apk
DefaultContainerService.apk	PackageInstaller.apk	colorservice.apk
DeskClock.apk	PicoTts.apk	framework-res.apk
DownloadProvider.apk	Push.apk	imssettings.apk
ExactCalculator.apk	QtiTelephonyService.apk	qcrilmsgtunnel.apk
ExtServices.apk	Settings.apk	webview.apk
ExtShared.apk	SettingsProvider.apk	
ExtraWallpapers.apk	StatementService.apk	
FusedLocation.apk		

Table 9: APKs extracted from an Encrochat BQ X3

BackupRestoreConfirmation.apk	ManagedProvisioning.apk
BasicDreams.apk	MediaProvider.apk
BlockedNumberProvider.apk	MtpDocumentsProvider.apk
Bluetooth.apk	Music.apk
BluetoothExt.apk	MusicFX.apk
BluetoothMidiService.apk	NQNfcNci.apk
CMFileManager.apk	NetworkSetting.apk
Calendar.apk	NvTerminal.apk
CalendarProvider.apk	OfflineCalendar.apk
CallLogBackup.apk	PacProcessor.apk
Capstone.apk	Packagelnstaller.apk
CaptivePortalLogin.apk	PhotoTable.apk
CarrierConfig.apk	PrintRecommendationService.apk
CarrierDefaultApp.apk	PrintSpooler.apk
CellBroadcastReceiver.apk	Protips.apk
Certlnstaller.apk	Provision.apk
CompanionDeviceManager.apk	ProxyHandler.apk
ConfURIDialer.apk	QtiTelephonyService.apk
Contacts.apk	SecureElement.apk
ContactsProvider.apk	Settings.apk
CtsShimPrebuilt.apk	Settingslntelligence.apk
CtsShimPrivPrebuilt.apk	SettingsProvider.apk
DefaultContainerService.apk	SharedStorageBackup.apk
DeskClock.apk	Shell.apk
Dialer.apk	SimAppDialog.apk
DocumentsUl.apk	SimSettings.apk
DownloadProvider.apk	SoundRecorder.apk
DownloadProviderUi.apk	StatementService.apk
EasterEgg.apk	Stk.apk
Email.apk	StorageManager.apk
Emergencylnfo.apk	SystemUl.apk
EventReceiver.apk	Tag.apk
ExactCalculator.apk	TeleService.apk
ExtServices.apk	Telecom.apk
ExtShared.apk	TelephonyProvider.apk
ExternalStorageProvider.apk	Traceur.apk
FusedLocation.apk	Updater.apk
Gallery2.apk	UserDictionaryProvider.apk
HTMLViewer.apk	VpnDialogs.apk
InputDevices.apk	WAPPushManager.apk
KeyChain.apk	WallpaperBackup.apk
LatinIME.apk	WallpaperCropper.apk
Launcher3QuickStep.apk	WallpaperPicker.apk
LegacyWipe.apk	framework-res.apk
LiveWallpapersPicker.apk	qcrilmsgtunnel.apk