IN THE INVESTIGATORY POWERS TRIBUNAL **IPT/21/37C**

Mr Nasar AHMED and others

v

National Crime Agency

Supplementary expert report of Professor Ross Anderson

I, Ross John Anderson, say as follows.

Instructions & material relied on in making this report

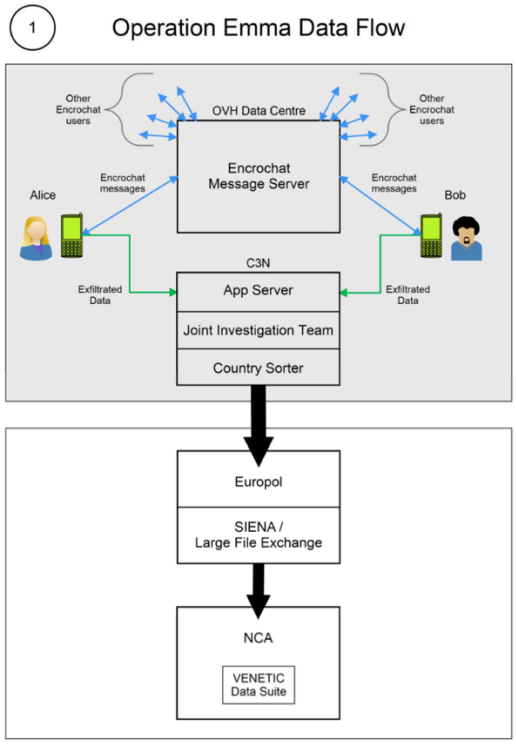
1. I have been provided with a further suspected EncroChat X2 handset and asked to provide an opinion on:

    a. The method of exfiltration of the material, including both metadata and message contents, from X2 and X3 handsets.
    b. Whether I have any comments on Luke Shrimpton's report of November 3rd on picture messaging.
    c. Whether the understanding of Emma Sweeting, as confirmed by Jérémy Decou, was necessarily wrong.

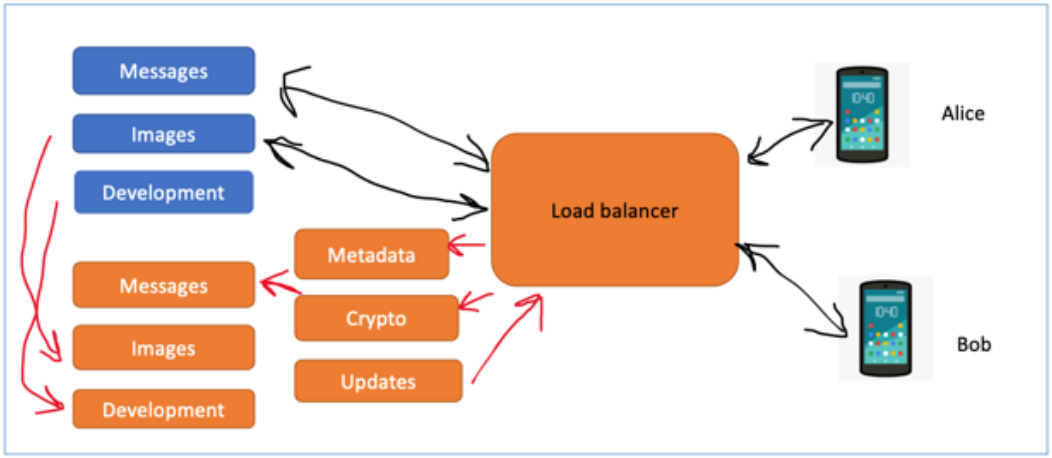
Previous opinion

2. The position of the NCA in respect of the phase 2 interception, which provided the bulk of the evidence offered in these cases, appears to have been that an 'implant' was loaded into the EncroChat handsets that copied message traffic and location data to a separate C3N server. Outgoing messages were copied to this server while stored in cleartext, as they presumably were before being encrypted for transmission, and incoming messages were copied after being decrypted and stored on the recipient handset, whether in volatile or nonvolatile memory.

3. This understanding is reflected in the Campbell report, a diagram from which I reproduce below. Two users, Alice and Bob, exchange messages via the EncroChat server which amounts to a substantially unmodified telecommunications system, while their handsets also have an implant, supplied by the JIT, which reports to a separately located C3N server.



4. However the technical evidence contradicts this model. The design of the EncroChat system required all the messaging and control traffic to and from the EncroChat devices to pass through the EncroChat cluster in Roubaix. The attack by the French and Dutch Joint Investigation Team (JIT) therefore modified many of the components of the EncroChat telecommunications system, and duplicating the others so that a version under JIT control could stand in for the original version. The phone software was changed to report substantially more data, and both the normal message traffic and the new data flowed to a load balancer. This could redirect traffic to any EncroChat service to a copy service controlled by the JIT. The diagram as I put it in my report of January 5th is as follows.



5. My opinion of January 5th was therefore that, according to the technical evidence, the operation undertaken by the JIT was a much more substantial and complex enterprise which involved taking effective control of substantial parts of the EncroChat telecommunications system. Access to message traffic involved not just decryption, but also the live interception of messages en route from the sending handset to the message server and from the message server to the recipient handset. I concluded that the attack amounted to interception. On this conclusion, the understanding of Emma Sweeting, as confirmed by Jérémy Decou, was necessarily wrong.

6. Since January 5th we have uncovered new evidence that significantly strengthens that conclusion.

New evidence

7. In what follows I will assume, to avoid repetition, that the reader is familiar with my report of January 5th. In it I discussed limited network experiments with an EncroChat Aquaris X3 ('Carbon') device. These were the newest phones offered to EncroChat customers and could not be compromised by the JIT at the start of Operation Emma; they were eventually compromised in June 2020. I reported that:

    a. 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;

    b. the X3 device did not leak either plaintext or cryptographic keys to the message server via the messaging protocol;

    c. we could not see how the device exfiltrated additional information such as its cellsite location.

8. That experiment re-used an experimental setup initially reported by the NCA's Luke Shrimpton to explore the correlation between actions taken by users of EncroChat devices and messages sent to and from the EncroChat servers. It had the limitation of only monitoring traffic using the same protocol (MQTT on port 8883).

9. Since then, we have built a testbed that enables us to monitor all attempted communications to and from a device under test.

10. We have also obtained a working EncroChat Aquaris X2, the older device used by most EncroChat customers, and which was exploited from the very start of Operation Emma in April 2020. Interception from conversations with an X2 at one or more of the endpoints therefore provided the vast majority of the electronic evidence available in the EncroChat cases currently before the courts.

11. We now have two working X3s, one working X2, and the original unmodified EncroChat app software disclosed by the NCA to enable us to replicate Luke Shrimpton's experiments. These samples enable us to explore the effects of the device compromise that followed updates of the EncroChat apps at various stages of Operation Emma.

12. We still have not extracted the modified EncroChat software from any of our working devices as these devices have been modified to make extraction difficult, as described in my report of January 5th. Software extraction risks device destruction and as we have only three working devices, we have done the network experiments first.

13. As I noted on the 5th January, the JIT / DGSI installed a load balancer in OVH Roubaix which intercepted the traffic from the EncroChat devices to one or more of the EncroChat servers; they also replicated the EncroChat infrastructure; and they got a warrant on March 4th 2020 to lock the Domain Name Server (DNS) for `encrochat.ch`. This restriction appears to persist; although the domain is listed as available, we have been unable to register it. We have however succeeded in registering the domain `zerolegacy.ch` that was used for the update server.

14. As I also noted, the architecture of the phase 2 live interception meant that when Alice sends Bob a message, it does not just flow from Alice to the messaging server (Sam) to Bob. It now flows from Alice to the load balancer, which we might call Louis, to Sam, and then once more to Louis, and then to Bob. And indeed we see in the evidence that incoming messages appear to be collected twice. They look as if an incoming message from Alice to Bob, as it appears in Bob's evidence bundle, has been intercepted by Louis en route from Alice to Sam, and a second time en route from Sam to Bob.

15. I also discussed how the message contents could be determined and mentioned several options:

    a. The first was that each handset just takes a copy of each message sent or received and sends it to the load balancer;

    b. The second was that the handset also sends each message contents in clear;

    c. The third is that the handset sends the load balancer every key it generates;

    d. A fourth is to send the key along with the message;

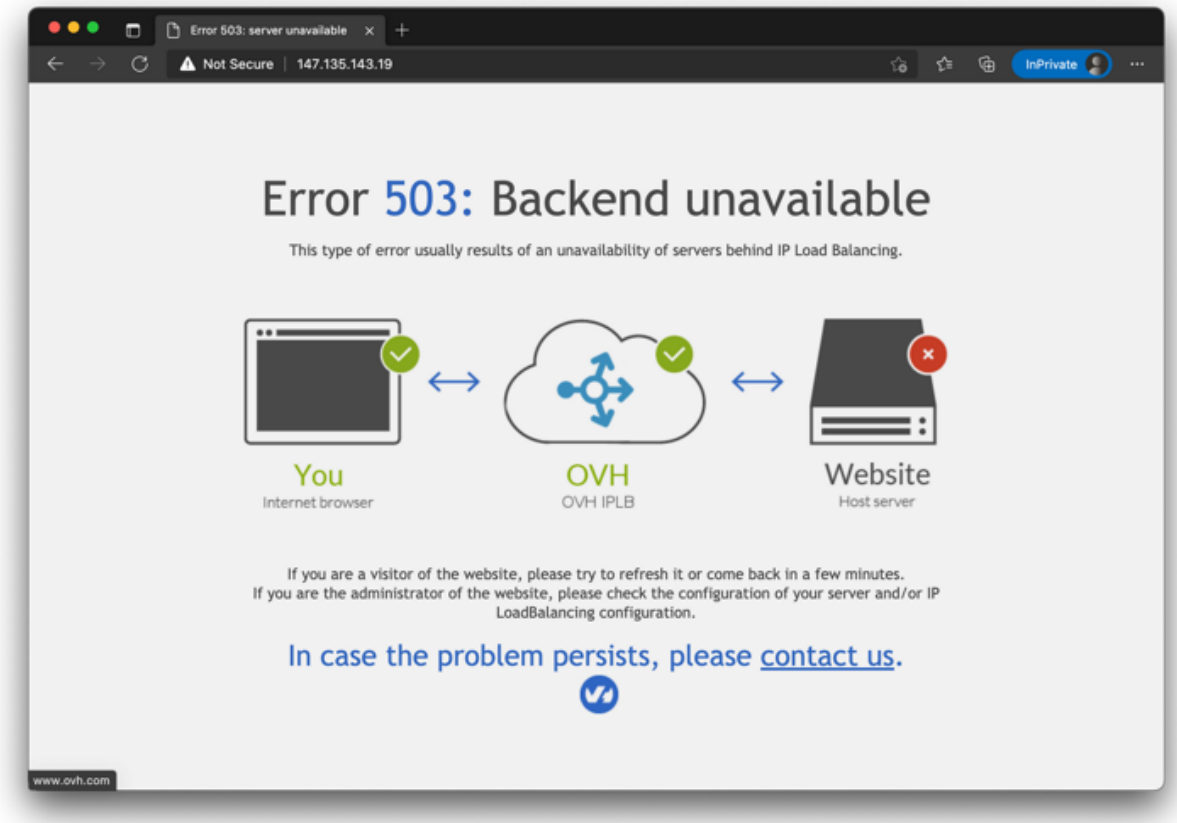
    e. A fifth is to interfere with the random number generator so that all the cryptographic keys are predictable by JIT / DGSI.

16. My assessment in June was that (e) above was the most likely. This is still possible but the new evidence we have collected since January 5th suggests (c) instead.

17. In the network experiments we reported then, test messages sent by an Aquaris X3 to out MQTT server did not result in any additional message traffic on port 8883. This suggested '*that if any of options (a) through (c) were used then the exfiltration was not done via the message server, or even using the MQTT protocol on which the original unmodified EncroChat app relied.*' I continued: '*This experiment does not rule out other means of exfiltration including a dedicated command-and-control server using a different protocol.*' I also noted that: '*These network experiments rule out a number of options but do not yet give a clear explanation of how location data, possibly keys, and possibly messages, were exfiltrated by the modified app via the load balancer.*'

18. Now that we have built equipment to observe all the message traffic to and from the device, we have made the following discoveries.

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.

24. Next followed a number of encrypted messages for other EncroChat users, in the XML format familiar from our report of the 5th January. These may have been messages composed by the device's erstwhile user but not transmitted before its last interaction with the service.

25. Next, a number of messages with the '<status>Alice</status>' tag were sent to different destinations including `gov.support@encrochat.com`. This may be a protocol to tell a user which other users are online. Curiously, each message has a 'presence ID' which is a GUID, a 256-bit apparently random value that might leak a cryptographic key, in accordance with 16(c) above.

26. Next followed a number of messages to `info.internal@encrochat.com` each of which contains an 'IQ ID'. In the XML message format used by EncroChat, an IQ (info/query) ID sets a context for communications with a device, and is typically followed by contextual information. In these messages, we see an IMEI field, a SIM field (which is blank; we had removed the device SIM card) and a GUID in the IQ ID field, which can be used to leak a cryptographic key, in accordance with 16(c) above.

27. We do not see any leak of plaintext to the MQTT server, or any communication to any other server. There is thus no visible means for the plaintext of the messages to be disclosed other than by decryption of the end-to-end encrypted ciphertext.

28. We would not expect to be able to verify directly whether the GUID in the IQ ID or the Presence ID contained a cryptographic key, as in such a 'key escrow' protocol it would be normal for the key being leaked to be encrypted using a key known to authority, in this case presumably DGSI.

29. The volume of communications from some 20,000 handsets to `info.internal@encrochat.com, gov.support@encrochat.com` and possibly a small number of other collection accounts established by the JIT and coded into the modified X2 app would have been substantial. With perhaps 50–100 messages per handset per day, mostly about location updates, over a million messages a day would have been directed to the MQTT message server; an increase in the traffic by about 20 transactions per second averaged over the day, and perhaps 100 transactions per second at peak times, would have been obvious. There appear to be only two reasonable options.

    a. The first is that the load balancer actively parsed the message stream from each device and removed from it all the extra messages so that they would not overwhelm the MQTT server and alarm the EncroChat administrators. In this case the collection of traffic from the updated X2 apps involved active interception of all message traffic at all times.

    b. The second is that the JIT took over the entire EncroChat operation from April 1st, locking the EncroChat administrators out. This had been a theory of at least one defence lawyer in these cases. I had considered it a lower probability scenario because the interception lasted for two months before the alarm was

raised, and because the interception was flaky, with numerous gaps in the collection. But then a senior officer from the Dutch National High Tech Crime Unit hinted in a public talk that they had completely taken over the system[1]. I am happy to entertain this account of things; a complete takeover of the infrastructure from day one (or later) would also amount to interception.

30. On the matter of image messaging, it was – and remains – my opinion that while images were collected by JIT from devices in the first phase, they were collected directly from the media server or servers in the second phase. The process of sending a message involves the sender encrypting the image, uploading it to a media server, obtaining a "downloadUri", and then sending both the downloadUri and the key material to the recipient. Here, "Uri" stands for Universal Resource Identifier, a generalisation of the URL familiar as an address from which to download material on the world-wide web. If the image is stored in the device, there may also be a "storageUri".

31. In his report of November 3rd, Luke Shrimpton relates an experiment with unmodified EncroChat handsets that appears to show that that the storageUri for an outgoing message is generated when a picture is taken, while for an incoming message it is created when the jpeg is downloaded or viewed. He claims this shows that images were intercepted from devices rather than being taken directly from the media servers. But to take just one example, the evidence disclosed for dottedjaw (the handle allegedly used by the claimant Nasar Ahmad) has in April 13th two intercepted images, 887f9335-0dd7-437c-b708-d8e1d8e29c5d.jpg and 26436b0f-cc10-4746-ac3b-7af1ae6ad659.jpg. The json files show the related messages from the handle swiftfax; in both cases there is a downloadUri but no storageUri (these are deb325e64d52fd7d2e2f1eb74a6a0e5773447385d599d0edb3688bafaf765869 and 5dc64c6fb70223eb592ca3fbe6d04476adb2841f7a0a143cbb8895943e7dd128 respectively). In fact I am unable to find any non-null storageUri values in any of the json line files of phase 2 intercepts disclosed to me. Mr Shrimpton's experiment thus rather substantiates my analysis that the phase 2 images were collected from the servers.

32. I therefore sharpen my conclusions from my report of January 5th, as follows.

    a. The EncroChat telecommunications system consisted of the EncroChat app, running on at least three different types of phone, plus a central infrastructure of 70-plus virtual servers at OVH.

    b. Interception involved unauthorised modification of the app and the replication of this infrastructure, with the addition of an active *'mesure de captation'* in the form of a load balancer to switch traffic between the genuine EncroChat servers and copies of them introduced for the purpose of interception.

[1] 'Hansa Market, Cyberbunker and EncroChat: The Security Practices of Organised Crime', Erik van de Sandt, Jan 14 2022, at https://www.cl.cam.ac.uk/research/security/seminars/archive/video/

c. All the data – even the phase 1 sweeps that were copied from handset Realm storage – were encrypted at the handset and then collected at the server infrastructure of this communications system which had been modified in this way. They were thus intercepted from the telecommunications system.

d. The intercepted material was collected through a load balancer operated by DGSI, the French internal security service, and aggregated on servers under its control. The phase 2 images were certainly intercepted from the media servers rather than from the handsets. Some of the message contents were probably obtained by decryption, particularly those received by X2 handsets. The X2 messages were intercepted in the sense that the JIT / DGSI used the load balancer to intercept them en route to the message server. The X3 messages were also intercepted in the sense that the JIT relied on the load balancer to collect them within the constraints of the EncroChat system architecture, namely a single TLS-encrypted IP stream going to the OVH data centre in Roubaix.

33. The concept of operations relied on by Emma Sweeting and which formed the basis of the IPCO warrant is implausible. Her understanding was necessarily wrong, and this fact is beyond reasonable doubt.

I understand that it is my duty to help the court understand matters within my expertise and that this duty overrides any obligation from the person from whom I have received instructions. I have complied with that duty and will continue to do so. I have done my best to be accurate and complete.

I confirm that I have made clear which facts and matters referred to in this report are within my own knowledge and which are not. Those that are within my own knowledge I confirm to be true. The opinions I have expressed represent my true and complete professional opinions on the matters to which they refer.

I understand that proceedings for contempt of court may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief in its truth.

Signed



Professor Ross Anderson FRS FREng

Cambridge, 8th February 2022