KCS Group Europe

Tales from The Encrypt

9th July 2020

A rare and seemingly supersized success for the UK's National Crime Agency, as EncroChat, an encrypted messaging system used by some of the top criminals in the country, is successfully cracked, resulting in over 700 arrests and drugs, guns and cash in significant quantities being seized. Although the full scale of this operation is unlikely to be publicly known, police chiefs and politicians alike have hailed it as a major blow for British organised crime for many years to come. However, things are unlikely to ever be that simple.

Amid the standard confiscation of assault rifles, cocaine kilos and bundles of banknotes, were some startling claims: that interception of messages on EncroChat revealed plots to torture, disfigure and murder members of rival gangs. This level of sustained activity and facilitation was only possible through a network such as EncroChat which, far from a typical encrypted WhatsApp chat, involved specially-adapted mobiles, messages that self-destructed after a set period of time, and the ability to permanently wipe the device's entire data core. Such a capability is worth rolling up in its own regard, regardless of the criminality it facilitated.

However, even when taking into account the individuals and networks who will be de-fanged as a result of these raids, EncroChat was assuredly only one tool in their arsenal. The very fact that such a network could exist, and with such capabilities for almost-immediate 'burning' of any sensitive information, sets a grave precedent for future policing action: the bad actors will adapt, and improve, upon the EncroChat product for next time, as new capabilities are wrung from the technology. Also, calling it a 'product' is entirely correct: this was a professionalized operation to market specific devices directly enabling criminal activity. Those behind EncroChat (based in France) may claim that they only supply the technology, the only illegal intent comes from the users, but this is semantics. Supplying technology to the criminal industry may be just as significant an industry in itself.

Two other factors to consider: that this was not a Dark Web operation (save perhaps, and this is remains unknown, for the procedure for buying the adapted Androids in the first place); the actual usage of the phones did not require any dark web or indeed any web presence at all, and the police themselves have admitted that 'luck' certainly played a role in the discovery and cracking of EncroChat. Any replicas then might also be operating even outside the Dark Web, long considered the standard repository for laundering, smuggling and general criminality. It may be that this solidifies a new front in the evolution of bad actors' techniques.

Secondly that this network was operating entirely irrespective of lockdown, indicative that the criminal activity continues despite the global situation (and may actually be enhanced by it). While EncroChat was used by British crime lords and gangs, any similar operation could be easily conceivably targeted at state-sponsored or industrial espionage concerns, and without that element of 'luck' who can say if they will be rolled up in the same way?

Added to this are the legacy issues from Apple's very public spat with the FBI in 2016, when the latter attempted to force to tech giant to unlock the smartphone belonging to a terrorist shot dead in the San Bernadino assault. The FBI eventually secured access through a third-party, but a legal order maintained that Apple could not be forced to comply in any case. Presuming a situation where an EncroChat-style device is recovered successfully, it remains to be seen how British law would interpret such a dilemma; but as always, inaction whether through lethargy or perceived morality tends to favour the criminals.

This is certainly a victory in battle, but the war may be so intangible in scope and so nebulous in its aims that it may represent a summit, rather than acting as a step along the way.