AFP / OPERATION KRAKEN

Law enforcement targeting of dedicated encrypted communications platforms

PHANTOM SECURE

EncroChat

SKYECC

ANØM

Ciphr

Phantom Secure
Dismantled 2018

EncroChat
Compromised 2018

SkyECC
Taken down 2018

AN0M
Disabled June 2021

CIPHR
Access changes 2021

In 2017, the AFP partners with the FBI and the Royal Canadian mounted Police (RCMP) to target the DECP **Phantom Secure** under Operation SAFECRACKING.

Phantom Secure was a Canadian-based business which developed sold DECDs exclusively to transnational criminal organisations, including those located in – and targeting – Australia.

The company sold a modified Blackberry phone that included a range of technical features designed for users to evade law enforcement detection. Including the ability for users to wipe content from the phone remotely.

Although at the time it was not the only DECP to exist, it was one of the premier solutions for criminal syndicates to communicate securely. At the height of Phantom Secure's popularity, there were about 20,000 users on the platform.

After Phantom Secure was disabled, criminals looked for other dedicated encrypted communication devices.

EncroChat was a communications platform that designed and developed a secure device with a customised operating system that had several communication applications.

Users of the EncroChat service purchased a modified Android handset from an Encrochat supplier along with a foreign roaming SIM. The device was modified to have two operating systems, one open and unsecured and another that was hidden and highly secured by a number of passwords.

EncroChat guaranteed their phones could not be traced.

In 2020, police in Europe, led by the Dutch and French, compromised EncroChat, allowing authorities to read messages. In June 2020, subscribers were told by EncroChat that the platform had been compromised and users were advised to get rid of the devices.

When Encrochat was compromised, criminals turned to other dedicated encrypted communications platforms such as SkyECC and AN0M.

SkyECC was an end-to-end encrypted messaging app originally for Blackberry devices, developed by Canadian-based company Sky Global. The application enabled self-destructing messages and was later developed for Android and IOS devices.

Before its takedown in 2021, SkyECC was the world's largest encrypted messaging network.

After suspecting SkyECC of enabling serious transnational crime, European law enforcement agencies covertly accessed the network. Content confirmed European law enforcement agencies' suspicions.

After the takedown of SkyECC in March 2021, many organised crime networks quickly sought a DECD replacement for SkyECC and one that would continue to allow them to securely carry out their criminal activities without law enforcement detection.

In 2018, the AFP and FBI were presented with the opportunity to develop, run and secretly access a dedicated encrypted communications platform called **AN0M**, through a human source.

The resulting police operations provided law enforcement with a unique and unprecedented ability to access to a platform used solely for criminality. Not only that, the AFP devised a technological solution to read the encrypted text messages between criminals in real time.

The AN0M app was uploaded on a smart phone and hidden behind a calculator app. The device looked like any normal phone, and if unsuspecting law enforcement seized one, it would look like there was no information or content stored.

AN0M was used solely by criminals, who were again attracted to a platform that had a range of features, including the ability to send encrypted text messages. No phone calls could be made and a number of other normal mobile phone features had been disabled.

Part of law enforcement's strategy was to organically get AN0M into the criminal underworld – this DECD was sold by criminals, for criminals. Within a year, serious criminals were vouching for AN0M.

For three years, the law enforcement sat in the back pockets of criminals, watching and listening to their illegal activity.

In June 2021, AFP's Operation Ironside went to resolution and AN0M was disabled.

In 2021, **CIPHR** was the most popular DECD active in Australia.

CIPHR offered a series of privacy-focused apps that the company installed on Android devices. They included CIPHR Text, which was an instant end-to-end encrypted messaging app; an email system called CIPHR Mail, and CIPHR Vault, which was designed to securely store files locally on the device. Resellers were able to sell devices with companies' software for thousands of dollars for a six month or annual subscription.

Following the successful resolution of AN0M in 2021, and almost as a sign that the CIPHR enterprise knew of its criminal clientele, CIPHR banned the company's resellers in Australia from providing service, which meant that Australian users were unable to renew their subscription to CIPHR.