Operation Greenlight Part 1: The International Sting

Introduction

Superintendent Ted Esplund

So this was a gold mine for us and we immediately saw the potential of this operation. And I think we pretty much made the best of it from day one.

FBI Special Agent Stephanie Stevens

Yeah, I'll stick with excitement, exciting. Everything was pertinent. It was overwhelming detail of prolific drug trafficking activity.

Head of the Organised Crime Unit at Europol Georgios Raskos

One aspect that I find particularly important is that intelligence coming from OTF Greenlight/Trojan Shield, but also similar investigations, was instrumental for law enforcement to trigger new cases.

Europol narrator

Welcome to the Europol podcast, the official podcast of the EU's law enforcement agency. In this series, we shine a light on some of the biggest operations Europol has supported, and how we continue to fight organised crime.

Operation Greenlight Part 1: The International Sting.

In a world where crime becomes more international, law enforcement can hit globalised criminal networks hard by taking out one of their most precious resources; their secure communication channels.

Georgios

In this regard, we see that criminals have a strong appetite for criminally dedicated, encrypted communication solutions. This allows them to coordinate their criminal projects, to remain in contact, manage their criminal networks while being far away.

Europol narrator

That's Georgios Raskos, Head of the EU Organised Crime Unit. He coordinated Europol's work on today's case.

Georgios

At the same time, this is an opportunity for law enforcement. Criminals need encrypted communication services to communicate.

Europol narrator

What are these opportunities for law enforcement? Let's look at some recent cases.

In early 2020, EncroChat was one of the largest providers of encrypted digital communication, with a very high share of users presumably engaged in criminal activity. A large dedicated team at Europol investigated, in real time, millions of messages during the investigation, and Europol provided analytical, technical and financial support for this case. French and Dutch law enforcement teamed up with Europol and Eurojust to take the platform down later on in 2020.

After that, many of EncroChat's users moved to a similar platform, called Sky ECC.

Sky ECC offered subscription-based encrypted communications for criminals, and reportedly over 150 000 Sky devices were in circulation at one point. Belgian, French and Dutch authorities conducted an enormous action that took the network down, and once again they intercepted countless messages and got plenty of fresh criminal intelligence to work with. Europol provided those national authorities with tactical, technical and financial support, and was dealing with the flow of information on criminal activities, thereby preventing major crimes and threats to life.

In this two-parter, we're looking at one of the most sophisticated law enforcement operations to date in the fight against encrypted criminal activities. It has many names – Operation Trojan Shield, Operation Ironside – but at Europol, it is called Operation Greenlight.

Investigation into Phantom Secure

Stephanie

I'm Stephanie Stevens, and I'm a special agent with the FBI.

Nicholas

And Nicholas Cheviron, special agent with the FBI.

Europol narrator

Stephanie and Nicholas are the FBI experts who led Operation Trojan Shield, the FBI's name for Operation Greenlight. And things began way back in 2016, with the demise of a company called Phantom Secure.

Nicholas

So we started an investigation against Phantom Secure in 2016 and at the time, Phantom Secure was sort of the name brand of these hardened encrypted devices.

Stephanie

There are multiple companies out there and they're constantly competing for the same criminal base.

Nicholas

We became familiar with these hardened, encrypted devices and that they were being used by tens of thousands of criminals around the world, primarily involved in large-scale international drug trafficking.

Europol narrator

Phantom Secure was a company selling phones that claimed to be untraceable. Criminals could use them to message each other, and law enforcement, in theory, had absolutely no way of knowing how the criminals were organising. And if law enforcement got its hands on your Phantom Secure phone, you could ask Phantom to remotely wipe it, removing any incriminating evidence inside.

Nicholas

And these devices are really just a secure mode of communication. So they look like a phone, but they don't act like a phone. You can't make typical phone calls on them. They're really just a locked down device that are absent many of the features that a traditional phone would have.

Europol narrator

And with the prices Phantom Secure were charging, it's pretty clear that most of us aren't the type of clientele that Phantom Secure were looking for.

Stephanie

So in order to have them, you have to pay upwards of USD 2 000 every six months just to have the subscription for the device. So beyond these features that a normal user wouldn't like - the absence of Instagram, Facebook, calls, the Internet - the price is fairly steep, and that's mainly due to the data roaming sims.

Europol narrator

Indeed, the FBI realised that Phantom Secure weren't marketing to normal people like you or me; their customers were serious organised criminals.

Relying on word of mouth, and offering free subscriptions to the right people, Phantom became a sizeable enterprise selling encrypted phones to dangerous organised criminals. But the law eventually caught up with its CEO, he was arrested, and he admitted to creating the device to help drug traffickers.

Phantom Secure's disappearance meant its criminal user base, which numbered in the tens of thousands, lost its secure network. There were also the lost users of EncroChat and Sky ECC, which we referred to earlier. Lots of criminals out there needed a new provider.

A small window had opened to launch an international sting; Operation Greenlight was about to begin.

ANOM devices

Europol narrator

Could law enforcement develop its own Phantom Secure-style encrypted device, market it to the criminals, and then snoop on the criminals using the devices to land convictions and save lives?

That's how Operation Greenlight worked. The FBI was to launch its own encrypted devices under the company name ANOM, and see if the criminals would take the bait.

Stephanie

ANOM was a competing encrypted communications device. It was an application that was modified by the FBI in conjunction with the Australian Federal Police.

We were able to leverage their expertise in the technological world and being involved specifically with these devices. And then we were able to help modify that with them. So

beyond building the company, the application, we also had to build a strategy on how we were going to deal with the data. But first we had to build a device that could compete, could operate, could function like these normal devices do, but also on the back end could be able for law enforcement to read and review the messages.

Nicholas

So we were doing all of the things that the competing companies were doing. We were just doing it from a covert aspect. We had to purchase hardware and Sims just like everybody else. We had to ship them to the countries that needed them.

We needed it to look as if the company was based outside of the United States. We needed to have a website like many of these other companies do, and so we were able to set that up.

Europol narrator

Another key consideration for the FBI was keeping normal citizens away from the devices. And they implemented means to prevent people like you or me from getting our hands on an ANOM device.

Nicholas

We didn't want this to just be commercially available. So even our website had a password that you needed to access it. So even if an everyday user knew, hey, I want to go search ANOM and I want to find it, if they were able to find the website, they needed to know a reseller who could give them the password so that they could get that information from the website.

Europol narrator

So the FBI's fake encrypted device, ANOM, was coming together – the paper trail was building up, the parts were being acquired and assembled, and now they needed to win the trust of the criminal networks who were previously using Phantom Secure and the other hardened devices.

Nicholas

So we knew, just get it to into the hands of a few influential people in the criminal underworld. And they'll sort of take it from there because they'll be driven by money, the money that they're going to make off selling these devices, money that they're going to be making from the criminal activities they're conducting on the devices.

Europol narrator

And let Nicholas and Stephanie tell you a little bit more about some of the features in these devices.

Stephanie

If you were able to open the device and see just the regular screen, you wouldn't see any of the normal applications that an everyday user would have. It would almost appear to be like a very plain burner phone. However, if you went to the calculator app and you clicked on that, that's where you could put in a password hold down the equals sign and then boom, you're in the ANOM application.

Nicholas

These are the kinds of things, one of many features that just didn't make sense to a normal everyday user, but they were specifically meant or built for the criminal user base, who do find value in that kind of feature.

There was also a feature that allowed you to put in a certain code that would essentially create a wallpaper that had some of those Facebook, Instagram applications on it. So that if you were ever questioned by law enforcement or you needed to sort of legitimise it and show someone you could do that.

Europol narrator

And that's not all.

Stephanie

We had a feature in the device that essentially worked like a push to talk so you could push and hold down the audio button and you could record a minute long voice memo for your friend in that you could change your voice, make it high or low. And of course that provided them with a little extra security in the fact that, OK, they're not hearing my true voice, but us as law enforcement on the back end had to find a way to toggle that back so that we could hear true voice.

And we did, so while they thought that they were protecting their voice, we were on the other side receiving that and hearing them in true voice.

Europol narrator

That's a pretty clever set of features to put on a phone you want criminals – and not normal people – to buy. And they bought it.

The first users came up in Australia, where high drug prices act as a magnet for international drug traffickers. And the drug traffickers there told their buddies to use ANOM too, so ANOM started growing exponentially in other countries.

Each time ANOM devices entered a new country, the FBI would start collaborating with the respective government if they could. Criminal intelligence soon began coming in, and Nicholas and Stephanie had to start working with the reams of data exchanged by the ANOM users.

Nicholas

It did range, but the trust that was built into these devices for the most part, there was overwhelming specificity.

Europol narrator

So while some ANOM users were harder to identify than others, the FBI had successfully got an ear in the conversations of thousands of organised criminals. At the peak of Operation Greenlight, they'd earned 12 000 users.

Stephanie

This wasn't just small levels of amounts of drugs. This wasn't your, you know, lower level criminals. These were your sophisticated, international, large TCOs that were operating across the world. So we saw lots of detail. We began to see these well-known, high-value,

some very violent drug traffickers that we've known for a while and some we haven't.

Gathering evidence

Europol narrator

Now the FBI were realising just how successful Operation Greenlight was proving. They were scoring crucial evidence against known suspects, but also uncovering dangerous people who'd been under the radar previously. Eventually the FBI were even able to understand slang, codenames, and other discretion tactics used by the criminals.

Nicholas

Yeah. I think while it was exciting, and it'd been a lot of hard work to sort of see it, you know, work. But that excitement was short lived. And it I think it quickly turned to responsibility that we had a lot of information coming in and now we had to figure out what to do with it.

Europol narrator

The FBI began building intelligence packages that they could then share with other countries' police forces, so that those police could handle the criminals in their respective jurisdictions. Cases ranged from violent crime, to drug trafficking, to political corruption.

Nicholas

What we heard time and time again from our partners was that they were able to build cases against some of their most significant targets that had been on their radar for a long time, but they hadn't been able to gather significant evidence to bring a prosecution. Without highlighting one or two, we heard that from numerous countries, and so to be able to build cases against those who have eluded law enforcement up until this point, I think it was a really big deal for us.

I think the thing that we took the most pride in was certainly mitigating the threats to life. You know, we did see a lot of sometimes very horrifying and explicit things either after an act had already been done or discussing an act leading up to, and there was a lot of pressure to act accordingly and mitigate that risk if we could.

And so when we'd hear, oftentimes we would hear of the users say, hey, look, the police came and talked to me about this this guy we were going to talk to. You know, how could they have known about that? It gave you a little bit of sense of relief that, OK, we've at least postponed that for a little while and that individual may not have known how close he or she really came to, you know, having some real violence enacted on them.

Conclusion

Europol narrator

And so that is how law enforcement pulled off one of the most impressive stings in modern policing. Dozens of countries working together, sharing intelligence packages built up via the ANOM encrypted devices, and hundreds of dangerous people being put behind bars.

Stephanie

The sole reason for the success of the operation was the fact that we built these relationships, started mostly bilaterally as we say. Those relationships, building those, it

did- it took a lot of time and it took a lot of balance, but it was the sole reason for the success.

What we realised is that we, the FBI team, couldn't have enough video conferences with these partners to help coordinate information so we started to see things like country A needed to talk to Country B, they were coming through us and we realised that it had almost gotten to the point that we were slowing down the flow of information and we all needed to be coordinating and on the same page.

Europol narrator

And the FBI realised that Operation Greenlight was ready to enter its next phase; a Joint Action Day coordinated at Europol headquarters. Law Enforcement from 16 countries were to converge on Europol headquarters, including partners such as the Swedish Police.

Ted

We were just starting the investigation phase with EncroChat and we have thought that this was once in a lifetime.

Europol narrator

Superintendent Ted Esplund joins us in part two, when he describes a case opened in Sweden as a direct result of Operation Greenlight. You will also hear about the Joint Action Days coordinated from Europol HQ, as told by the agents who were in charge.

Georgios

I think that we cannot highlight enough that the information that an investigations like Greenlight/Trojan Shield are offering to law enforcement are precious for law enforcement. It has a unique value as intelligence and as evidence to be used for ongoing investigations, but also to be used for initiating, for triggering new investigations in the participating countries.

Europol narrator

Thank you very much for listening. If you enjoyed the show please rate, review and subscribe to us on whatever platform you're using, and tell your friends about the show if you think they'll enjoy it too.