Crime Interrupted
An AFP and Casefile Presents podcast.
Episode 2, Operation Boone transcript.

Host – introduction
The Australian Federal Police – or AFP for short – is Australia's national policing agency. Its aim? To – outsmart serious crime with intelligent action. Officers from the AFP work with local, national, and international agencies to combat serious criminal threats. Their work includes counter terrorism, serious organised crime, human trafficking, cybercrime, fraud, and child exploitation. The AFP exists to disrupt major criminal operations. In 2020-21, they did that over 400 times. They seized 38 tonnes of illicit drugs and precursors, and assisted overseas police services in seizing 19 tonnes of drugs. The AFP charged 235 people with child exploitation, and charged 25 people following terrorism investigations.

We've got exclusive access to the AFP case vault and personnel to provide you with in-depth insight into how they investigated and interrupted the most serious of crimes to stay a step ahead.

Host
Operation Boone had an unusual beginning. One of the AFP's Cybercrime officers travelled to Pittsburgh in 2018, to attend a worldwide conference about cybercrime. The conference ran for six weeks, and for the experts from around the world, much of their discussions were about trends in cybercrime. When an FBI agent heard an AFP officer was in attendance, he approached her and passed on intelligence the FBI had picked up about a website called WickedGen.com. The site was used to sell stolen usernames and passwords for services like Netflix, Spotify and Hulu for a fraction of the subscriber cost, so people could access these sites illegally. FBI intel concluded that the person operating the site lived in Australia. When she returned home from the conference, the AFP officer relayed the FBI information to her team, and they decided to take a closer look.

AFP criminal intelligence analyst, Dale Redfern, says the case began when a high school teacher in the United States overheard some kids talking about how to get cheap subscriptions online.

Dale Redfern (3.12)
I have to say, this is probably one of the most unusual ways to start an AFP investigation. The information that was related to us by the FBI was that there was a group of school kids, in Iowa, in a high school, talking in the playground about getting cheap Netflix. A teacher overheard them, thought it was a little bit unusual. Reported it up the school chain. They then told the State Police. They then told the FBI, and then all of a sudden, it became this national and international investigation. Very unique start to a very interesting matter.

Host
In essence, an offender in the United States was hacking into businesses and stealing usernames and passwords. Because so many people use the same username and password for everything, it means this data can be sold, and chances are, the username and password you used to log into your coffee loyalty card will allow a thief to log into your Netflix account.

In this case, an Australian offender had purchased sets of stolen usernames and passwords from the US hacker. The hacker had sold the stolen credentials in bulk, not knowing if the passwords worked. The Australian buyer then had to figure out which sites he could match to the stolen username-and-password pairs. He would run the pairs across various sites like Netflix, Spotify, and Hulu to find matches. The Australian offender then sold those username-and-password pairs on a website called WickedGen on a large scale. So, a customer could buy the login details to Netflix for a fraction of the cost they would normally pay for a legitimate subscription. The money earned was being filtered into a complex system of PayPal accounts. Once the AFP Cybercrime team started investigating the Australian offender doing this, Operation Boone was born.

Dale Redfern (5.14)
In this case, the information was provided by the FBI. And it did identify an account generator site called WickedGen. From that preliminary investigation, the FBI gave us a handful of PayPal accounts that they had identified were receiving payments as part of the WickedGen payment platform.

Host
We asked Dale about the role of a criminal intelligence analyst when information like this comes forward?

Dale Redfern (5.41)
The role of a criminal intelligence analyst within the AFP is to interpret the criminal environment, and provide timely, relevant, and actionable intelligence. It can be tactical. You might have a phone number. You might have an email address. You might have a person. And it's trying to work up a profile and understanding of that person and their role as a criminal essentially. You also have a more strategic aspect of things, how do they move the money from A to B? Are they using technology? Are they using encryption?

Host
In many cases, the role of an analyst starts before a criminal investigation is launched. With the complex web emanating out from the WickedGen site, Dale Redfern would be kept very busy, trying to uncover the extent of the offending.

Once Operation Boone began, AFP investigator, Senior Constable Joanna Kondos came on board as the case officer. Joanna had joined the AFP after doing a degree in Maths at university. She was drawn to law and order, loved structure, and saw the AFP as having an analytical investigative focus. After joining up and doing a stint at the airport, Cybercrime seemed a natural path for her.

Joanna Kondos (7.03)
So, in January of 2019, I had joined Cybercrime after spending some time in uniform at Sydney Airport. I had been in the AFP for probably about just short of four years at this stage, and chose to come to Cybercrime because it was something that was growing. This industry was not something that was ever going to slow down. And it was exciting that it was an area of the AFP that was really gaining some traction. So, I'd just joined Cybercrime. I was new. There was definitely no prior skillset or knowledge from me in the tech world, but it was a challenge.

Host
For an officer who loved problem solving, Operation Boone was going to provide her the perfect opportunity to help unravel a hugely complex and carefully concealed cybercrime.

Joanna Kondos (7.59)
After completing an internal cybercrime course, just to get me over the line of knowing some of the terms of references, I joined this team, and on their books, they actually had Operation Boone. So I became aware of the job through a briefing from the case officer at that time, who ended up handing over the job to me a short time later, and on the forefront learnt that there was an individual located in Australia who was the author and administrator of something called an account generator website. I'd never heard of account generator websites. I had to do a little bit of my own research and found that these websites actually sell other people's usernames and passwords to services. So, it's a way that an individual can pay a little less to get a service.

Host
The AFP discovered that this illegal trade in stolen usernames and passwords was big business.

Joanna Kondos (8.59)
The website that was the main focus at this point of the referral was called WickedGen. So WickedGen was selling other people's subscriptions to services such as Netflix, Hulu, Spotify. In fact, there were over 50 different types of services that it was offering. And the site itself prior to its shutdown claimed to have over 120,000 users. So it was fairly popular. And I thought it was interesting that I'd never really heard of these kinds of websites, but clearly other people had. They offered a cheaper price to these subscriptions. So whilst you and I might pay $11.99 a month for a Netflix subscription, it was being offered on these sites that you could pay $2.99 a year or $4.99 for life. But what were you actually buying was someone else's username and password, not a subscription through the legitimate site itself.

Host
So, because most people use the same username and password over and over, there are easy and automated ways of testing it against other sites. The process is called 'credential stuffing', where large numbers of username-password credentials are automatically entered into a target website. The ones that match existing accounts can then be sold by sites like WickedGen.

Joanna Kondos (10.22)
Because it's automated, it means you can throw hundreds of thousands of pairs through a script in no time. And what you're left with is a list of successful credentials at that stage that will gain you access on behalf of someone else that hasn't given you access. You can, even though it's unauthorised, actually gain access into their account. So, I guess what this does is it preys upon that vulnerability of human nature, that sense of keeping a single easy to remember password across multiple domains, across multiple platforms and services, it's something that we all do. These days, you need a password to access almost everything, so traditionally the easiest way to do that was to have something that you remembered and then add your capitals or numbers or special characters. What this kind of process does in credential stuffing is it works around that.

Host

Operation Boone began with some good old-fashioned web searching. The AFP team was in luck when they found that someone on YouTube had done a review of the WickedGen website and jumped through the hoops as a customer. The way it worked was all there, laid out for the investigators.

Joanna Kondos (11.47)
Sometimes it's actually nice that the public can do a little bit of our job for us, in this sense, present us a YouTube review of the final iteration of account generator websites that our offender was responsible for. And what this really gave us as investigators and intelligence analysts was that customer perspective, the walkthrough of the site from the purpose of the customer in making a purchase. So whilst it was nice to see what it visually was able to look like, it was also good to see the service options. So, the Netflix, the Spotify, the Hulu, the NBA, UFC. But then even more so as this individual on YouTube stepped through the purchase, it also showed us the payment page. And then from that, we were able to see the payment options. So very quickly, we became aware that there wasn't only PayPal as a payment option, but there was cryptocurrency too. And that adds a whole another element to this case, because it's not just cash anymore. It's not just bank accounts. It's not even now just PayPal. We have that added element of cryptocurrency. So, it kind of better armed us in knowing what we were dealing with when we did come to the point of identifying the offender, was that we were aware that there was a high likely opportunity here, that there was cryptocurrency involved and that takes a little bit more work.

Host
A bonus for investigators was that the YouTube review video showed the reviewer clicking through to the PayPal payment option and the sale page showed the account the payment was going into.

Joanna Kondos (13.32)
The YouTube review showed this individual generating the account. So they've made the purchase, so now they literally press on a button that says 'generate account' and up pops a username and a password. And they even showed going to the Netflix site and putting in that username and password, and it gained them access to someone else's Netflix account. It had that typical page that we all see with the four or five names of the users of the single Netflix account, none of which were the person that was actually using it. And they click in and they have full access to that person's Netflix account.

Host
What was interesting was that when the AFP did their own investigation, the PayPal payment account shown on the YouTube review had changed.

Joanna Kondos (14.20)
I guess, something that was interesting for us in comparing this review to our analysis of that website, was we were able to see that there's something set up in the background of this website that means that for some reason, at the time of this review, it went to a certain account, and then when we did our own, it went to another account. So it stepped up that understanding that there was a level of sophistication to the backend of this website, which allowed for it to service people, the way that it did.

Host

And this switching payments between accounts became another avenue of enquiry that would turn out to be bigger and more sophisticated than anyone imagined.

Once the AFP confirmed that WickedGen was selling stolen usernames and passwords on its site, they used all of the usual ways to try and track down the person running it. We've all seen it on films – the police try and trace an IP address, but the hacker has routed it through other addresses. This was exactly what the AFP found when they tried to trace the location of the WickedGen website. Tracking the account was made more difficult because some of the services the site was using were from overseas.

Joanna Kondos (15.40)
A big task of ours as investigators is to identify what's in the backend. So what services are being used to allow for this website to actually operate, whether it be proxy servers, whether it be the domain hosts, whether it be any other technical service that allows for the use of a website. When we were doing this, we found that there were a multitude of email accounts that even though they related to the one website, all the services were registered in different accounts. Something that was common amongst them is that they were registered in GMX and Gmail accounts. So GMX is a service running out of Germany. And Gmail is of course, Google running out of the US. By going to these entities and requesting information, based on these accounts that we'd identified, we were finding that a lot of the IP addresses linked to these accounts led us to VPN servers. And it was leading us down a path that required a fair bit of resources to try and crack through. What we relied upon here was these offshore entities working with us to link these accounts.

Host
We hear about people using VPNs. But what actually are they?

Joanna Kondos (17.05)
VPN is a virtual private network, which is a way that an individual can essentially obscure their location. A VPN service is used to make sure that the site in which you're sitting on does not know where you are located. So, it's a bit of a barrier in between, for your anonymity.

Host
The AFP always works with, and relies on the cooperation from, organisations all around the world. In Operation Boone, Google proved really helpful.

Joanna Kondos (17.42)
Rather than requesting information on individual email accounts, we could go to them with a group of them and say, where are these linked and how are these linked? And in the case of Google, they provided some incredible analysis of the cookies linked between the different accounts. Every time you jump on the internet, and you perform some searches, you leave a trace, and this is in the form of a cookie. So, these cookies in relation to all of these accounts, ended up having some links. And that was a really good way for us to be able to link all these different registrations to a single entity.

Host
Because it was the FBI who first brought the Australian Federal Police into the case, AFP Cybercrime in Australia teamed up with the FBI in a parallel investigation which gave them

opportunities to share information. The weight and might of the FBI also opened doors for the AFP.

Joanna Kondos (18.44)
Having the FBI work on this and having their expertise as well as ours just meant that all of a sudden I had available to me as the case officer, the full realm of technical ability from investigations to intel analysts to technical specialists and beyond, and anything that we received throughout the course of the investigation, all the way through to resolution, we were able to work on together, and bounce off each other in terms of ways, in which to really open up this investigation and identify the realm of criminal activity.

Host
When you watch cybercrime investigators in movies, there's always an expert who works magic on the computer, doing things that regular people can't. But for Joanna and her team, utilising readily available open-source materials to investigate, worked just as well – especially when one email kept coming up over and over again.

Joanna Kondos (19.47)
A common email address came up throughout the course of the investigation and what we were able to do through open-source intelligence is have a look at the clear net and the dark net in seeing where else this comes up. So sometimes it's a matter of piecing the puzzles available together to create the picture of crime. And in this case, it also assist us in being able to put a face or a name or username to the individual that's actually behind the computer screen.

Host
When Joanna talks about open-source intelligence, it means it's freely available online. One site that is worth a visit is the *Have I Been Pwned* website which tells you if your email address has been compromised in a data breach. The AFP combined their technical capabilities with these online open-source intelligence sites and found something important – the offender's first name.

Joanna Kondos (20.51)
When we had a look at the open source materials that were available to us, we found that this email address of interest was coming up in forums, where anyone's available to comment on whatever they like. And in one case, we actually had an angry message to this user,' [beep] you.' And then the name of our offender. So, it was interesting that if we were working towards the identity of the offender, we now have a name that potentially we can match to other identifying features of this investigation.

Host
Piece by piece, the mystery of the unknown Australian offender started to unravel. A chance mention of his name was just the beginning.

The complexities involved in Operation Boone were vast. The man behind the selling of data had done a good job of hiding. But it's almost impossible to leave no footprint in cyberspace. The offender himself had used the same username over a number of sites when commenting on forums. And that was what the AFP Cybercrime team was counting on. For intelligence analyst, Dale Redfern, it meant tracking thousands of posts.

Dale Redfern (22.13)
The offender had so many posts online. Literally thousands upon thousands. On one of these forums, the offender was a prolific user. He had posted over 2000 times over six years spending the equivalent of 10 weeks logged into the site. There was literally a plethora of insight into him, his actions, and his associates. But there were many other forums: Black Hat World, Bitcoin Talk, Knolled, The Bot, Whirlpool, Twitter; it goes on and on and on. That's not even to mention the endless gaming sites. Each of these sites provided an understanding of his conduct, his location, his behaviour, and his interests. But the difficult part – you have to review every single post. You don't know whereabouts in these thousands of posts, you are going to find that gold nugget. You don't know what is going to be relevant at the time. You don't know what might come 500 posts in the future. You don't know how it might link to add another digital bread crumb in another site. It's a matter of collecting, collating, and analysing that data, stitching it all together to fill intelligence gaps from which we can pivot.

Host
It was in one of these forums, the offender revealed his age and location. And it would turn out, he was very young.

Joanna Kondos (23.36)
In another forum, we had identified that the offender had actually posted and said, 'I live in New South Wales.' And then after a few more comments said, 'I live on the Northern Beaches.' And at that time, was 15 years old. So we're now starting to put a picture of this real human being, to the activities of someone behind a computer.

Host
That post was from several years earlier, so it meant the offender was 21 at the time of being investigated. Joanna herself wasn't that much older than her quarry.

Joanna Kondos (24.10)
At this time, I was not that much older than the offender at 25. And I think there was a bit of a personal reflection piece here that how interesting that we both had an interest in that mathematical problem-solving space of the world. Yet I chose a path down the line of law enforcement and he's chosen a path down the line of criminal activity. And that it didn't really matter what our upbringing was, what school we went to, whether we have the same socioeconomic status, at the end of the day, you either choose to do good or you choose to do something that's not so good. And in this case, at that fork in the road, he's chosen the wrong path, and that's led him to being investigated by the AFP.

Host
The offender in Operation Boone – who we will refer to as 'Jim' – left crumbs behind that the Cybercrime team followed. Criminal intelligence analyst Dale Redfern kept digging. He soon discovered the extent of the PayPal accounts the offender was using.

Dale Redfern (25.23)
What quickly became apparent was that the names and details on those PayPal accounts were fake. They all had Sydney addresses. They all had very similar email addresses, but not a single person could be identified as being real. They had mobile phone numbers attached to the email accounts and to the PayPal accounts that were fake, or if they weren't fake, they were assigned to persons who had absolutely no role whatsoever in PayPal or with the WickedGen account. Whoever had set up these accounts was disciplined, coordinated, and

had covered their tracks. Well, almost. So, the first port of call was to take a deeper dive into the PayPal accounts. I did not appreciate at the time just how much work was going to be involved.

Host
Worldwide, there's a lot of debate about whether pineapple goes on pizza. Who would have thought that ordering pineapple on pizza on a PayPal account could bring the AFP closer to the offender?

Dale Redfern (26.26)
So there's really very few leads for which we could actually pursue. But there was something odd on just one transaction. On one of those accounts, out of the 150 odd accounts, there was a single line, a PayPal transaction to a Domino's Pizza. We thought that's a little unusual. We didn't know where it was. Obviously, Domino's is a bit of a global brand, but we dug a bit deeper. About two and a half years earlier in 2015, there was a PayPal order that purchased a Hawaiian, a Supreme, and a vegetarian pizza, all to be collected from a Domino's store on Sydney's Northern Beaches. I remember sitting there wondering: *who puts pineapple on a pizza*? But seriously for us, there was something in the Northern Beaches.

Host
The irony wasn't lost on the investigators that Jim was leading them right to him because he too used the same username across multiple platforms.

Joanna Kondos (27.24)
I guess, a common mistake that he made, that he was preying upon when it came to the human nature of using the same passwords and same usernames across multiple platforms, he'd actually done the same thing. The same names did keep popping up. Every new inquiry led to a new email address or a new username. But at the end of the day, they were then linked to another username or email address that we already knew about. Everything linked to something else. And really that's where we could put together this web of information for which our offender was smack bang in the middle of it.

Host
While WickedGen was the original referral from the FBI, there had been a few iterations. The first one was HyperGen but it had been shut down a couple of years earlier. Investigators in Operation Boone found out that HyperGen had been hacked in May 2016, and the entire customer base, ironically, had been dumped online. AFP investigators discovered an online dump – or full copy and paste – of the HyperGen database.

Joanna Kondos (28.36)
The AFP actually located a copy of that HyperGen database online, and something that is of interest to us in the case of HyperGen, is that usually the first registered user of a website, which is subscription-based, is that the first user is usually the administrator themselves. You can't set up an account without checking it yourself. So when we were able to locate this, and we call it an online dump or it's a paste of that database, that admin user, as the first registered user, came back to an IP address, which subsequently ended up being the home address of the offender, subscribed in his father's name.

Host
Once they got that close, the Cybercrime team were able to find Jim on social media platforms. On Instagram, they finally got a visual of the man they sought. He had posted a photo of himself doing a muscle flex in a mirror. According to his profile, he was a young man still living at home. He did not have a lot of followers.

Joanna Kondos (29.51)
You check their socials because someone's socials be it Instagram, Facebook, Twitter, it's a real window into someone else's personal life. You see what they like, you see what they post, you see what their interests are. And in this case, it actually led us to our offender's Instagram. And there it was, a post of our offender standing in a mirror with his phone, having a flex. And it really was the first time I laid eyes on the person that I thought, wow, okay. This is the guy that we've been investigating for so long. And this is the person behind all of this criminal activity online and sophistication. And he was standing in front of a mirror with his tank top, with his headphones on, and kind of trying to portray to be the cool dude. And, at the end of the day, we were aware that he actually spent a lot of his time at home on his computer. So, it kind of did that stereotypical contradiction of what we portray to society versus who we are behind closed doors. He didn't look very old. He didn't have much facial hair, and he really did look like a kid, and this really hit home that this person has incredible ability yet they're choosing it to cause harm rather than using it for good.

Host
The investigators from Operation Boone built the case around the young offender. One thing that is hard to do in cybercrime is to hide the money trail. Subscribers around the world were paying him electronically. Jim had come up with an ingenious and complex way of juggling and hiding payments. He had used a number of unverified PayPal accounts, and it was through them that he was collecting the money.

Dale Redfern (31.52)
At the time that the offender was using PayPal, PayPal had an exemption from the Australian financial regulator. As long as the balance kept under that thousand dollars, you were fine. If however, you went over that a thousand dollars PayPal would ask the customer to provide their full ID – a driver's license, a passport, a bank statement, some form of identification that would confirm your true identity. If you didn't, PayPal would freeze the accounts and you would not get your money. It made life very hard for the offender. Because, what that offender had to do was to ensure that his balance each time was less than $1,000. It required almost a full-time attention to ensure that his account balance across his multiple accounts did not reach that thousand-dollar mark. He would have spent hours a day trying to rearrange, transfer funds, move funds around from A to B, from B to C to ensure that he did not reach that limit.

Host
And this wasn't just a couple of accounts. The Cybercrime unit would eventually identify over a hundred accounts that the offender was juggling to keep them all under the $1,000 limit.

Dale Redfern (33.04)
As we went through the PayPal accounts, over the months ahead in fact, we trawled through all the PayPal records; we trawled through the money flows. The five accounts quickly became 10, 20, 50, a hundred. Hundreds and thousands of lines of PayPal data were collected

and analysed. Purchases, log-in details, IP addresses, transfers to and from, a whole range of other PayPal accounts, also in fake names, also at fake addresses. It quickly became one entangled mess. Almost all the accounts were unverified. All-in-all, a customer base somewhere in excess of 150,000 users, and had subscriptions ranging from $3 to $30. And of those about 85,000 of his customers were paid customers. Doing some very simple maths, there is a fair amount of money being made. The size and scale was simply unprecedented.

Host
Jim had developed a new site called AutoFlix which only sold Netflix. It showed he was reading what the market wanted.

Joanna Kondos (34.15)
Our offender had identified that the most popular service was Netflix. And so, because this was the most popular, he actually ventured into a specific account generator website called AutoFlix that purely sold Netflix accounts and whilst it bubbled away and didn't earn as much money as the other account generator websites, it definitely was a constant form of income. What it meant is he just preyed upon the popularity. So he was able to see a market, reach the market, and build something for that market.

Host
Eventually, Jim found he had a problem that legitimate businesses would love to face. Suddenly, the demand for his services was too high and he shut down WickedGen in 2018. Not only that, he couldn't handle the support tickets lodged on the site when customers suddenly found they couldn't log onto the service they'd paid him for. This would happen if the legitimate user cancelled their subscription or changed their password.

Joanna Kondos (35.25)
WickedGen, which was going at the same time as AutoFlix actually was no longer active as of January 2018. And something that we were able to piece together was that there was a number of unsolicited advertisements for this website that had been published online. So people had seen the site, seen that it works, how cheap it was, and how successful it was, and decided to do some advertising on his behalf. It's interesting that advertising can actually be a downfall. And in the case of WickedGen, it was. The site became so popular that there was an incredible surge in popularity that actually led to he didn't have enough accounts to service the amount of customers.

Host
It's easy to think of the crimes Jim was committing as victimless, but the truth is, the victims were regular people innocently subscribing to services, whose credentials were being sold. If someone can get access to your Netflix account, they can see what you've been watching, know what you're interested in. And they have your username and password. What would stop them trying to use it to access your email or for other invasions of privacy?

Joanna Kondos (36.49)
What were you getting out of the service at that level of then not being able to show your hand to the victim, that you were inside, in their service. So like the example of Netflix, of watching a movie or watching a series, the person then who legitimately owns the account, the unknowing victim, do they log on and see that someone started watching a show that you have no interest in whatsoever? Or, did they see that whilst they pay for three accounts, they keep getting a notification that they're on too many accounts at once. It's almost an invasion

of your privacy, right? That someone is able to jump onto your account and see what you're interested in, see what you're watching. And was there a way that our offender could ensure that the people buying the credentials were not using it for other purposes? No way. He's definitely not going to stop someone with a criminal intent in using a victim's credentials for purposes beyond what he was offering as a service. The email and password, whilst it's being sold as my Netflix credentials, it could also be the credentials to my bank account, to my superannuation, to my government Centrelink account. And then all of a sudden, this victim is now being exposed on a level way greater than a service that can help you stream movies or music.

Host
Over the course of the investigation, Jim was also developing his skills in industry. His fourth and final account generator website showed his level of sophistication and skill development was growing.

Joanna Kondos (38.35)
AccountBot was the final iteration of account generator websites. It was the last of the four. And by this stage, our offender had really become quite sophisticated in the way in which they have developed their website. So no longer was it required that anyone manually check all of these accounts. What was set up was this automation with AccountBot that at the backend of this website, at the single point that a customer wanted to generate an account, it was set up that this website would check that account there and then against the target website, and only provide it to you in the event that it was a successful login. In the event it wasn't a successful login, the website was programmed to get the next account and check that. So there was this real upgrade in the work behind the websites and the customer experience that this was now going to allow for less manual labour, for less support tickets, because it was checked that these accounts were actually useful before being given to your customers. I guess the other thing that it also did was it meant that people weren't generating more accounts than they'd paid for. So, in the event that someone had changed a password and the account was no longer accessible as a customer, I would come back onto the website, onto AccountBot, and I would request the website to get me a new set of credentials. The site was set up so that it didn't just get me a new set of credentials. It actually checked the ones I'd already been given, just to make sure that they actually were no longer successful in the access, before giving me a new one. And again, checking that new one before I received it. I guess, from a business sense, what that allowed him was the sense that no one could just keep generating accounts and saying that they weren't working. His system checked up on that.

Host
Despite his caution and his complex management system, what brought Jim unstuck was that there were PayPal accounts that linked to his bank accounts. The AFP worked closely with PayPal to uncover this. It became a spider's web of accounts that came back to him. PayPal gave the AFP access logs to the 186 PayPal accounts that Jim was running. Just how long did it take criminal intelligence analyst Dale Redfern to sort it out?

Dale Redfern (41.25)
To unravel the whole web of the PayPal accounts took months. It took many, many meetings with PayPal. It took many, many meetings with banks and other financial institutions to trace money, and to trace funds and to find linked accounts. Some of these accounts used by the offender do not go to a bank or a financial institution. It went onto prepaid, preloaded, Visa

and MasterCards. Tracking down all the money, where it went, how it went offshore, was complicated, and required the assistance of many agencies.

Host
Once the AFP identified the accounts that the money was being funnelled into, they discovered that four Australian IP addresses were accessing these accounts. Finally, they had a common user. It was a pocket modem – or dongle – that belonged to Jim. Originally, it had been used with multiple SIM cards subscribed using false details, making tracking by law enforcement difficult. But over time, he became careless. Later he subscribed to SIM cards using his full name, address, and date of birth. It was a stroke of luck that there was a lag – or drop out – in the connection between VPN accounts. In this lag, the connection defaulted to Jim's pocket modem. And for nine seconds, he was not under the protection and anonymity of VPNs. He was logged on as himself.

Joanna Kondos (43.04)
When 99.9% of our IPs came back to that, our intelligence analysts found that there was a nine-second lag in a VPN connection, which came back to a Vodafone network, which at that stage also aligned with the alleged offender that we believed was behind these sites. And that nine seconds came back to the Vodafone Wi-Fi dongle that was being used in accordance with the offending, came back to the individual with his name, his address, and his date of birth. So that was a big win for us and an important when, in so much data, it can be this tiny lag in service that can actually be a little bit of an unravelling in a criminal activity.

Host
Once Operation Boone identified Jim and tracked the extent of his cybercrimes, the operation moved to the arrest stage. And it was not going to be an ordinary arrest. The FBI agents who had worked with the AFP, came over to take part.

Joanna Kondos (44.12)
So, it was really special for us to be able to actually invite the FBI special agents to attend the warrant with us. Not only because they had worked so hard on this investigation with us for such a period of time, not only because they were the referring agency, but also because they had this knowledge and skillset, which matched ours in terms of this particular investigation. Many hands make light work. So having everyone there meant that there was, there was more scope and knowledge of this investigation as a whole. And in what world would you ever say no to leveraging off that? So to have them here in Australia, it was something that we were able to share with them, and that was really special.

Host
Even though it was a cybercrime, Joanna Kondos and her team made the decision to call in the tactical team to make the arrest. They're the scary-looking ones dressed in black.

Joanna Kondos (45.14)
In this case, it was decided that our specialist support team, or a tactical unit, were to make the entry when it came to this search warrant, and a fair bit of consideration was given to this. It's probably not very common that you would think that a cybercrime search warrant is met with a tactical team. But it is extremely important for us that we were able to make a rapid containment. And that just means get everyone in the right place, all the devices untouched, as quickly as possible, because at the end of the day, whilst we had, all of our information and our evidence available to us prior to that day, that laptop, his phone, they were really key

in this investigation. And so to have them unharmed, untouched, untampered with, was really important to the success of the brief of evidence before the court. I'm sure it was the biggest shock of his life, a young guy sitting on his computer, on his lounge, to get the shock of the tactical unit. But it was really important for us as an investigations team to ensure that that went without a hitch.

Host
Jim's dad got the shock of his life at the sight of the AFP tactical unit smashing in his door.

Joanna Kondos (46.36)
So his dad was at the location as well. And this was probably the first time his father had ever realised that his son, who's capable of so much, was actually using it to aid criminal activity. And I think that when you're talking about a 21-year-old offender who still lives at home, who we're alleging has earnt hundreds of thousands of dollars, it's a fair shock to your dad when the police aren't only knocking at your door, they're breaking it down.

Host
Jim was taken into custody and gave a no-comment interview. He was refused bail and spent three days in a New South Wales correction facility. It was all very well to sit online and develop websites that earned hundreds of thousands of dollars, but to be arrested by the tactical response team, then end up in a cell, was a harsh reality that the young man might never have imagined. After meeting him, Joanna felt he would not do well in jail.

Joanna Kondos (47.43)
I can't imagine being a 21-year-old, who's interested in cyber and that tech world, what it could have been like to be at the corrections facility for three days. To be surrounded by people that you would never have associated with, people under the influence of drugs and alcohol, people with a level of violence. For essentially a clean cut 21-year-old, this would have been a massive shock and probably the scariest time of his life.

Host
Luckily in the forced entry, the AFP got to Jim's computer before he could do anything to compromise the data. It turned out that the laptop was the Pandora's box of information. The 21-year-old was charged with five offences.

Joanna Kondos (48.41)
The very obvious offence here is to cause an unauthorised access to restricted data. Restricted data, being something that is protected by passwords in this case. So by accessing these accounts, he was actually committing an offence. The next one was to do with the money, and that is dealing with proceeds of crime, which we alleged at this point was greater than a hundred thousand dollars. That's actually a 20-year offence, which is quite heavy and quite daunting for a 21-year-old to be facing. So, another offence that we were able to charge him with, which is something that was a little bit less common and something we hadn't actually seen used in a criminal space before, was a copyright offence. So, by providing this service to services that were legitimately being provided by Netflix and Hulu and Spotify and NBA and so on, he was actually committing a copyright offence, so that had a maximum penalty of five years. And then of course, to get around all of the PayPal and money restrictions, when it came to the money laundering offences, we have that he gave false and misleading information to a reporting entity because PayPal in itself is a reporting entity according to the

AMLCTF Act, the Anti-Money Laundering and Counter Terrorism Financing Act. So all up, he was really seeing a fair bit of pressure in terms of the amount of offences he was committing. And also the level of these offences and how strong we believed the brief of evidence was for all five of these counts.

Host
When Jim was arrested in March 2019, the police confiscated cryptocurrency worth $460,000. On October 19, 2021, the Supreme Court of NSW ordered the forfeiture of all items of property to the Commonwealth, including cryptocurrency, and funds held in various bank accounts and PayPal accounts. As a result of the orders, approximately $1.6 million worth of property was forfeited to the Commonwealth. It was the largest forfeiture of cryptocurrency achieved at the Commonwealth level to date. Jim pleaded guilty to all charges. Given that he was so young at the time of his arrest, his lawyer argued for a non-custodial prison sentence.

On the 23rd of April 2021, he received a custodial sentence of 2 years and 2 months to be served by way of Intensive Correction Order, as well as 200 hours of community service. In sentencing, the judge said that the offender was not motivated by money, but rather the tech challenge of seeing how far he could take things. The judge offered the following advice: 'You can still do so much in your life that can be so beneficial for society.'

Joanna Kondos (51.58)
Our offender being served an intensive correction order, it is technically a custodial sentence, so it is as in the eyes of the law, it is as serious as serving the time in a jail. However, you serve at home or at a location specified with your justice representative, and you live in the community, but with some very strict boundaries, some very strict rules, and in the case that you breached that, you are then deemed to not be suitable to serve it by that way, and instead, you would have to go into a jail. You're not free. You're definitely not free. You are serving a custodial sentence; you're just serving it at home, with some pretty strict guidelines. It's something that was touched upon in the sentencing procedure by Judge Pickering was that this should really serve as a turning point in the life of the offender. And that whilst they have this ability and this skillset, use it for good. Use it to assist a business or a company or your own company, not for a criminal adventure, and not just because you can, it's not a good enough excuse in our world is: I did it because I could. And just because you have the ability doesn't mean you should. So, in this case, we had a young individual with an incredible skillset, preying upon human nature and making money out of selling other people's information, yet he should be using that skill elsewhere. And maybe for the better of the world, rather than for the better of himself.

Host
In the two-year cat-and-mouse investigation, Joanna Kondos wonders if people really understand the crime. For her, the bottom line is: theft is theft, regardless of whether of you do it in person, or from your computer. You can't sell what's not yours to sell. For her, the true victims were the everyday subscribers.

Joanna Kondos (54.10)
Something that really hit home to me was I got asked once who was my victim. And I think the way that this job was grasped by media was, someone's selling Netflix and Spotify and

Hulu and these big streaming services are being ripped off because someone's selling someone else's subscriptions for a cheaper price. And yeah, maybe the offender did cut Netflix from the ability of having all of these subscribers. But for me, what it came down to was that these accounts belonged to our everyday mums and dads on the street, unknowing victims around the world that had no idea that someone else was sitting on their account. And for me, it was those mums and dads, it was the young kids who spend that money that they have on their services; they were my victims. Absolutely. We were working on behalf of everyone, but it came down to these hundreds of thousands of subscribers that had no idea that that were being leveraged to make some money.

Host
Agencies like the AFP and the FBI are tasked with keeping cyberspace safe. Not only do they catch offenders like Jim, they also inform industries of areas they can improve on. Joanna Kondos takes pride in the fact that PayPal removed the process that allowed Jim to exploit and trade in unverified accounts. It was never meant to be a point of vulnerability, and as soon as the AFP alerted PayPal, their cooperation was swift.

Jim was very good at what he did. But the AFP was better. Catching an offender like him is at the heart of what the AFP Cybercrime unit is all about.

Joanna Kondos (56.03)
It all comes back to that sense of wanting to sit behind your computer and do something that you think no one knows about. And what our job is in Cybercrime is to make it known that we do know about it. And we can actually attribute you to the actions that you take sitting behind your screen.

Host
And for Joanna, unravelling the labyrinth of Operation Boone was a perfect example of the kind of job that drew her to the Australian Federal Police in the first place.

Joanna Kondos (56.35)
What was so exciting about this world of cybercrime was this ability to kind of break down the barriers of anonymity, was this idea that through all the resources available to us as an organisation, that we were able to almost break down that idea that people in this world can't be caught. That they live behind their computers and behind these identifiers that aren't themselves. And we can actually put a real human being behind the actions of online offenders. That was probably the most exciting part of cybercrime. It wasn't something I knew, it wasn't something I had a skill set in, but it was something that really aligned with the whole problem-solving notion that I really got excited about when joining AFP in the first place.

Host
Serious crime is getting seriously complex. To stay a step ahead, the AFP is recruiting those with diverse skillsets and backgrounds – just like AFP personnel Dale and Joanna and the roles they played in interrupting the illegal subscription service rorting consumers as part of Operation Boone.

After all, it takes all kinds to solve crime. With more than 200 roles across the organisation, in Australia and across the globe, you could help the AFP stay a step ahead too. Consider a career with the AFP.