AFP
AUSTRALIAN FEDERAL POLICE

Sydney man sentenced for selling online subscriptions using stolen credentials in international investigation

Saturday, 24 April 2021, 3:24pm

A 23-year-old Sydney man was yesterday handed a two years and two months' sentence, to be served by way of an intensive corrections order, for his involvement as the creator, administrator and primary financial beneficiary of a number of online subscription services which relied on stolen credentials from Australians and others around the world.

The man, who has also been ordered by the court to serve 200 hours of community service, was arrested in 2019 following international cybercrime investigations by the Australian Federal Police (AFP) and Federal Bureau of Investigation (FBI).

The investigation began after the FBI referred information to the AFP, in May 2018, regarding an account generator website called WickedGen.com.

WickedGen operated for approximately two years selling stolen account details for online subscription services, including Netflix, Spotify and Hulu. The account details were confirmed through a process of credential stuffing, which allows a list of previously stolen or leaked usernames, email addresses and corresponding passwords re-used and sold for unauthorised access.

The account details belonged to unknowing victims in Australia and internationally, including the United States.

Throughout the investigation, the AFP further identified the Sydney man to be the creator, administrator and primary financial beneficiary of a further three "account generator" websites; HyperGen, Autoflix and AccountBot. Across the four subscription services, the offender had at least 152,863 registered users and provided at least 85,925 subscriptions to illegally access legitimate streaming services.

The man received at least AUD $680,000 through PayPal, by selling subscriptions through these sites. He converted some of these proceeds into various cryptocurrencies.

On 12 March, 2019 the AFP executed a search warrant at Dee Why, on Sydney's northern beaches and seized the laptop which was used to run the operation and around AUD $35,000 in cryptocurrency.

The man was charged with unauthorised access to (or modification of) restricted data, dealing in proceeds of crime etc. – money or property worth $100,000 or more, providing a circumvention service for a technological protection measure, dealing in identification information and false or misleading information.

On 9 December 2020, the AFP-led Criminal Assets Confiscation Taskforce (CACT) obtained restraining orders under the *Proceeds of Crime Act 2002* (Cth) over various assets, including cryptocurrency, bank accounts and Paypal accounts.

The combined assets of the restrained property has a current value of approximately AUD $1.65 million.

The AFP-led CACT was formed in 2011 as part of a multi-agency crackdown on criminal assets, bringing together the resources and expertise of the AFP, Australian Criminal Intelligence Commission, Australian Taxation Office, Australian Transaction Reports and Analysis Centre, and Australian Border Force.

Together, these agencies trace, restrain and ultimately confiscate criminal assets.

The 23-year-old man has been sentenced to two years and two months to be served by way of intensive corrections order, as well as 200 hours of community service.

AFP Commander Chris Goldsmid, Cybercrime Operations, said the operation relied upon hacked credentials of millions of people around the globe.

"The harvesting and selling of personal details online was not a 'victimless crime' –these were the personal details of everyday people being used for someone's greed," Commander Goldsmid said.

“These types of offences can often be a precursor to more insidious forms of data theft and manipulation, which can have greater consequences for the victims involved.”

“This investigation is an example of the importance of our relationship with the FBI. These partnerships are critical to law enforcement being able to respond to a rapidly-evolving crime type.”

“We would also like to thank the affected companies for their cooperation with the investigation.”

The matter was prosecuted by the Commonwealth Director of Public Prosecutions.

Deputy Director of the CDPP, Mark de Crespigny said “This case demonstrates the ability of the police and prosecutors to unravel and address sophisticated transnational cybercrime.”

Information security is vital for individuals and companies. For more information visit the **Australian Cyber Security Centre’s website ‹https://cyber.gov.au/›** .

Media enquiries

AFP National Media: (02) 5126 9297