Police say hacker concealed ID in Australian privacy breach

September 30 2022, by ROD McGUIRK

An Optus phone sign hangs above its store in Sydney, Australia, Thursday, Oct. 7, 2021. Australia's federal and state governments on Wednesday, Sept. 28, 2022, called for Optus to pay for replacing identification documents including passports and driver's licenses to avoid identity fraud after 9.8 million of the telecommunications company's customers had personal data stolen by computer hackers. Credit: AP Photo/Mark Baker, File

The computer hacker who stole personal data of almost 10 million customers of a telecommunications company in one of Australia's worst privacy breaches used techniques to conceal their identity, actions and whereabouts, police said on Friday.

Australian Federal Police Assistant Commissioner Justine Gough, who heads cyber investigations, said the international probe, that includes the U.S. Federal Bureau of Investigation, into the Optus cyberattack last week would be "long and complex."

"You can be assured that our very clever and dedicated cyber investigators are focused on delivering justice for those whose personal information has been compromised," Gough said.

The government blames lax cybersecurity at Optus, Australia's second-largest wireless carrier, for the theft of current and former customers' personal information.

Cybersecurity Minister Clare O'Neil described the crime as "quite a basic hack." She said Optus, a subsidiary of Singapore Telecommunications Ltd., also known as Singtel, had "effectively left the window open for data of this nature to be stolen."

Optus maintains it was the target of a sophisticated cyberattack that penetrated several layers of security.

Gough declined to say whether the crime fitted the description of "sophisticated" or "basic."

"I'm not going to go into the details as to the attack because ... it is subject of our ongoing investigation," Gough said.

"But I would say that whoever is behind this attack has used obfuscation

techniques to conceal their identity, their location and their activity," she added.

While details of 9.8 million Optus customers were stolen, authorities are most concerned for more than 10,000 customers whose records were dumped on the dark web on Tuesday as part of an extortion attempt.

The hacker later withdrew a $1 million ransom demand in a post that apologized for the crime and claimed that all the stolen data had been destroyed. Experts are skeptical.

Gough declined to say whether any further extortion attempt had been made.

But she announced police forces throughout Australia had combined resources to "supercharge" the protection of the 10,000 who are most vulnerable to identify theft and fraud. Police are also working with the finance and services sectors to detect fraud.

"Customers affected by the breach will receive multijurisdictional and multilayered protection from identity crime and financial fraud," Gough said.

Operation Guardian will eventually extend to the next-most vulnerable tier of customers, the 2.8 million who have had their driver's license and passport numbers stolen.

Prime Minister Anthony Albanese said Optus had agreed to pay to replace the passports of compromised customers.

"I think that's entirely appropriate," Albanese said.

be published, broadcast, rewritten or redistributed without permission.