Australian police probe purported hacker's ransom demand

September 27 2022, by ROD McGUIRK

A customer waits for service at a Optus phone store in Sydney, Australia, Thursday, Oct. 7, 2021. The Australian government said on Monday, Sept. 26, 2022, it was considering tougher cybersecurity rules for telecommunications companies after Optus, the nation's second-largest wireless carrier, reported personal data of 9.8 million customers had been breached. Credit: AP Photo/Mark Baker, File

Australian police were investigating a purported hacker's release of the stolen personal data of 10,000 customers of the nation's second-largest wireless carrier and demand for a $1 million ransom in cryptocurrency, the company's chief executive said Tuesday.

The Australian government has blamed lax cybersecurity at Optus for the unprecedented breach last week of the personal data of 9.8 million current and former customers.

Jeremy Kirk, a Sydney-based cybersecurity writer, said the purported hacker, who uses the online name Optusdata, had released 10,000 Optus customer records on the dark web and threatened to release another 10,000 every day for the next four days unless Optus pays the ransom.

Asked if the hacker had threatened to sell the remaining data if Optus did not pay the $1 million within a week, the company's chief executive, Kelly Bayer Rosmarin, told Australian Broadcasting Corp., "We have seen there is a post like that on the dark web."

Australian Federal Police said Monday their investigators were working with overseas agencies, including the FBI, to determine who was behind the attack and to help shield the public from identity fraud. Police declined further comment Tuesday as the investigations were ongoing.

"They're looking into every possibility and they're using the time available to see if they can track down that particular criminal and verify if they are bona fide," Bayer Rosmarin said.

Kirk wrote in his website Bank Info Security that Optusdata later deleted the post along with three samples of the stolen data.

Optusdata sent Kirk a link to a new post that withdrew the ransom demand, claimed the stolen data had been deleted and apologized to

Optus as well as its customers.

"Too many eyes. We will not sale (sic) data to anyone," the post said, adding that Optus had not paid a ransom.

Kirk said he asked why Optusdata had changed their mind but received no response.

Australian Information and Privacy Commissioner Angelene Falk, the national data protection authority, said the latest post "indicates ... this is a very fast-moving incident."

"It's a major incident of significant concern for the community. What we need to focus on here is ensuring that all steps are maintained to protect the community's personal information from further risk of harm," Falk said.

Web security consultant Troy Hunt suspected the apology had come from the hacker. But he did not accept that the data was now safe.

"The question now is what happens next? Will we just hear no more from this individual? Will the data appear in a larger volume tomorrow, next week, possibly years from now?" Hunt said.

At least one of the 10,000 Optus customers whose data was released on the dark web Tuesday had received a text message purportedly from the hacker demanding a 2,000 Australian dollar ($1,300) ransom, Nine Network News in Sydney reported.

"Your information will be sold and used for fraudulent activity within two days or until a payment of AU$2,000 is made," the text said, including details of an Australian bank account in the name Optusdata.

The extortion target, identified only as Belinda and described as a mother of a 5-year-old child with cancer, told Nine, "To be honest, it's just not what we need."

"I guess they're just trying to hopefully pressure people into paying," she said. Nine did not report whether she intended to pay.

Earlier Tuesday, Kirk said the released personal data appeared to include health care numbers, a form of identification not previously revealed publicly to have been hacked.

Cybersecurity Minister Clare O'Neil urged Optus to give priority to informing customers of what information had been taken.

"I am incredibly concerned this morning about reports that personal information from the Optus data breach, including Medicare numbers, are now being offered for free and for ransom," O'Neil said. "Medicare numbers were never advised to form part of compromised information from the breach," she added.

O'Neil on Monday described the hack as an "unprecedented theft of consumer information in Australian history."

Of the 9.8 million people affected, 2.8 million had "significant amounts of personal data," including driver's licenses and passport numbers, breached and are at significant risk of identity theft and fraud, she said.

Kirk said he used an online forum for criminals who trade in stolen data to ask Optusdata how the Optus information was accessed.

Optus appeared to have left an application programming interface, a piece of software known as an API that allows other systems to communicate and exchange data, open to the public, Kirk said.

The Australian Financial Review newspaper said the theory that Optus "left open an API" had been widely reported.

Bayer Rosmarin rejected such explanations, but said police had told her not to release details.

"It is not the case of having some sort of completely exposed API sitting out there," Bayer Rosmarin said.

O'Neil didn't detail how the breach occurred, but described it as a "quite a basic hack."

Optus had "effectively left the window open for data of this nature to be stolen," O'Neil said.