The Optus data breach occurred through an unprotected and publically exposed API. This API didn’t require user authentication before facilitating a connection. A lack of an authentication policy meant anyone that discovered the API on the internet could connect to it without submitting a username or password.

Security Flaw #1

Three security flaws can be identified in this setup. The first is a public-facing API (Application Programming Interface. An API should never be public-facing if it facilitates access to sensitive internal data or permits interactions with core business operations. Examples of open APIs that follow best API security practices are the Google Maps API and the Weather API. Any data that's available through these APIs is completely isolated from core business processes, so it’s impossible to cause a data breach through these open APIs.

*Is your organization at risk of a data breach?*[*Click here to find out*](https://www.upguard.com/instant-security-score)*.*

Security Flaw #2

This brings us to Optus’ second security flaw. The open API facilitated access to very sensitive customer data. To get a sense of the level of sensitive data this API was granting access to, whenever an Optus customer loads their account information either via the Optus mobile app or the Optus website, an API such as the one that facilitated the data breach is used to complete the request.

Backend processes call upon sensitive customer records to load a customer profile. This is why the Optus data breach resulted in the compromise of the following types of personal data:

* Driver’s License numbers
* Phone numbers
* Dates of birth
* Home addresses

[According to an analysis](https://www.wsws.org/en/articles/2022/10/06/afrq-o06.html) of public Domain Name System (DNS) records by security analyst Jeremy Kirk, this unsecured API was likely public-facing and, therefore, accessible to anyone on the internet for up to three months.  
‍

[[](https://www.upguard.com/security-report/optus)](https://www.upguard.com/security-report/optus" \t "_blank)

See how your organization's security posture compares to Optus'.

[View Optus' security report.](https://www.upguard.com/security-report/optus)

‍

Security Flaw #3

The third and final security flaw in this vulnerability package was the use of incrementing customer identifiers. In the digital world, programs identify customers by a unique sequence of numbers and letters. These are the identifiers that are called upon when a customer loads their account. According to best cybersecurity practices, each customer identifier, or contactID, should be completely unique and unrelated to other identifiers to prevent hackers from discovering the formula that determines each customer ID.

In Optus’s case, all customer identifiers differed by an increment of 1. So if one customer had the unique identifier 5567, the next customer in the database could be found with the identifier 5568.

When a hacker gains access to a customer database, the first thing they do is cross their fingers and check whether data identifiers increase incrementally. If this is the case, brute force techniques aren’t necessary, and the process of stealing data becomes much easier.

When the hacker responsible for the Optus breach gained access to the company’s customer database, they were very pleased to find that all customer records were indeed stored with incrementing identifiers. This allowed them to write a script that requested every customer record in the database by simply incrementing each contactID index by one.

With virtually the entire data exfiltration process outsourced to an automated script, the hacker was able to complete the data breach much faster and at a much larger scale than it would have other been possible if unique customer identifiers had been used.

With virtually the entire data exfiltration process outsourced to an automated script, the data breach was completed much faster and at a much larger scale. This unfortunate efficiency led to the Optus breach becoming ranked as the second-largest data breach in Australian history.

During the entire period these three vulnerabilities were active - which is likely to be three months - 9.8 million Optus customers were always at risk of compromise through a domino effect of mounting exploitation severity. All that was required to initiate the breach was for a cybercriminal to eventually discover this perfect domino stack, and give it just one gentle push

“Optusdata” told Information Security Media Group reporter Jeremy Kirk they had acquired the data through an unsecured Application Programming Interface (API), which allowed access to Optus’s customer database from devices anywhere on the public internet.

The hacker was able to access the information of all of the company’s customers by running an automated script that asked for database records one-by-one, simply increasing the “contactId” index number by one with each request.

“Optusdata” explained that no username, password or authentication token was required, writing to Kirk: “No authenticate needed. That is bad access control. All open to internet for any one to use.”

APIs are used extensively to allow communication between different pieces of software, within a single device or across networks. When Optus customers view their account via a mobile app or the web, a similar API to the one that was breached is used to retrieve and display their own information. Properly implemented, this is only possible after logging in, and cannot be used to display the details of other customers.

Security experts have speculated that the exploited API was a new version that was being tested and was not intended to be accessible from the public internet. To protect security, such an API should have used test data rather than actual customer details.

Kirk’s analysis of public Domain Name System (DNS) records—essentially the internet equivalent of a phone book—suggests that the unsecured API may have been accessible for up to three months.

The massive breach points to the danger of placing sensitive data in the hands of vast corporations, whose only concern is profit. While the Optus data breach is notable for its vast scale, hacks accessing substantial amounts of personal data are increasingly common.

Reports suggest Optus had an application programming interface (API) available online that did not require authorisation or authentication to access customer data.

“In the instance, where a public API endpoint did not require authentication, anyone on the internet with knowledge of that endpoint [URL] could use it,” said senior manager of cyber security consulting for Moss Adams, Corey J Ball.

“If that endpoint was used to access customer data, then anyone on the internet could have used that endpoint to gather customer data.

“Without technical controls for authentication and authorisation in place, any user could have requested any other user’s information. The attacker likely scripted the process to repeat requests from the endpoint until they had collected millions of instances of personally identifiable information.

Optus still hasn’t confirmed how the data was accessed. It maintains the attack was sophisticated, but the home affairs minister, Claire O’Neil, has said the vulnerability was akin to Optus leaving a window open.

**Optus Data Breach Timeline**

Current as of Wednesday 28th September 2022–11:00am.

When events like the Optus Breach take place, it can often be difficult to follow along to all that is taking place, now that it appears to have calmed somewhat, I felt it might be beneficial to share a timeline and some notes I have been keeping of the event since it started on Thursday the 22nd of September.

**TLDR:**

· Optus suffered a cyber-incident; this was not a ‘sophisticated’ cyber-attack. It was a data breach. Likely on Wednesday 21st September.

· Up to 11.2 million past and present Optus customers are likely impacted.

· The Threat actor responsible for stealing then advertising the data released 10,200 records before claiming to delete the rest of the possible 11.2 million records. Optus did not pay the demanded $1 million USD ransom.

· The fall-out for Optus has been swift and dramatic with customer outrage and government displeasure openly discussed in the media.

· This is Australia’s largest data breach in terms of volume of citizens impacted, with Drivers licenses, Passports and Medicare numbers all difficult to replace.

· Despite the Threat actor claiming to have deleted the data they still had possession for over 7 days so we must assume that all 11.2 million customers data have been exposed.

· This breach will result in ongoing issues for customers involved. Fraud, spam campaigns, phishing attacks and even possible physical impacts are all possible due to the nature of the exposed data.

· Australian organizations and citizens can expect additional attention from cyber criminals in the coming days and weeks as the media attention around Optus continues.

For the timeline I will provide a headline and link for further review, I will include images and comments (in italics) only when they provide situational awareness.

**Thursday 22nd September 2022**

In the early afternoon the Australian broke the story releasing an [**article**](https://nam12.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.theaustralian.com.au%2Fsubscribe%2Fnews%2F1%2F%3FsourceCode%3DTAWEB_WRE170_a_TWT%26dest%3Dhttps%253A%252F%252Fwww.theaustralian.com.au%252Fnation%252Fmillions-hit-in-major-optus-data-breach%252Fnews-story%252F335ba2236d8f304ed447fbb325e6829f%26memtype%3Danonymous%26mode%3Dpremium%26v21%3Ddynamic-groupb-test-noscore%26V21spcbehaviour%3Dappend&data=05%7C01%7C%7Cc572a84881604cac2e8c08daa07e1e51%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637998760824735156%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=%2FCFaIUoc52VrnPOUetw1xuwg1UYtr2HLOtACCou3VK0%3D&reserved=0) about a cyber-attack at Optus and alleged that over 2.5 million customers data had been stolen.

Optus after the Australian article released a[**statement**](https://nam12.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.optus.com.au%2Fabout%2Fmedia-centre%2Fmedia-releases%2F2022%2F09%2Foptus-notifies-customers-of-cyberattack&data=05%7C01%7C%7Cc572a84881604cac2e8c08daa07e1e51%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637998760824735156%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=Cb%2Fielly2UL%2F8yO2W1U8swCXHCrPWCHK9dckMEZi%2ByA%3D&reserved=0) on their website about the alleged cyber-attack. This has been updated since Thursday 22nd September.

*The current narrative was that this was a ‘highly sophisticated’ attack, and that Optus was unaware of the extend of the exposure of the network by the threat actor.*

The [**OAIC**](https://nam12.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.oaic.gov.au%2Fupdates%2Fnews-and-media%2Foaic-statement-on-optus-data-breach&data=05%7C01%7C%7Cc572a84881604cac2e8c08daa07e1e51%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637998760824735156%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=onK0uPxi7dDorC75w5A2fROlJvhtPHWWFcOa5T9is7s%3D&reserved=0) released a statement that Optus had informed them of the breach. At this stage it was anywhere between 2.5 million and 9 million customers impacted.

It was now widely reported across [**media outlets.**](https://www.smh.com.au/technology/sophisticated-attack-optus-hackers-used-european-addresses-could-be-state-linked-20220923-p5bkfn.html)

**Friday 23 September 2022**

The [**Optus CEO**](https://nam12.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.news.com.au%2Ffinance%2Foptus-ceo-delivers-emotional-apology%2Fvideo%2F2da2cee7bf2c6e07af3bfcc76ef06830&data=05%7C01%7C%7Cc572a84881604cac2e8c08daa07e1e51%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637998760824735156%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=sHyH%2F9G0m2GQgdjZnQOBy8031FBUkrvuDG2U2yznaCQ%3D&reserved=0)held a press conference with the media and offered a formal apology to the public.

There was considerable [**customer backlash**](https://nam12.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.sbs.com.au%2Fnews%2Farticle%2Foptus-faces-a-customer-exodus-calls-for-compensation-amid-anger-over-leaked-data%2Fmw79n7avs&data=05%7C01%7C%7Cc572a84881604cac2e8c08daa07e1e51%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637998760824735156%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=7FjymK6OtwG22q0iOoX6seHQ5NsGX%2FhsH0AeGHpbaPA%3D&reserved=0)as customers were not notified prior to the media release on 22 September.

The [**ACSC**](https://nam12.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.cyber.gov.au%2Facsc%2Fview-all-content%2Falerts%2Foptus-notifies-customers-cyberattack-compromising-customer-information&data=05%7C01%7C%7Cc572a84881604cac2e8c08daa07e1e51%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637998760824735156%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=skhLzPrSmAkJhnM1U6F7O20B3vfIE929uL7nm%2BQdnSc%3D&reserved=0) released a statement and a ‘what to do next’ for Optus customers.

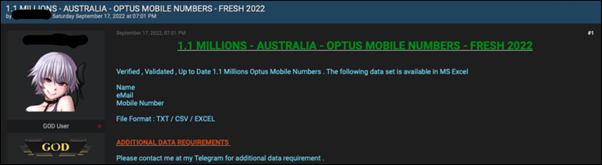
Optus reported that the hackers used [**European IP addresses**](https://nam12.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.smh.com.au%2Ftechnology%2Fsophisticated-attack-optus-hackers-used-european-addresses-could-be-state-linked-20220923-p5bkfn.html&data=05%7C01%7C%7Cc572a84881604cac2e8c08daa07e1e51%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637998760824735156%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=tbQIaNmeky8Iu6%2BBacBv6XepuB%2FD7%2Fe9ZnI1ujwHLaA%3D&reserved=0) and they could be state linked according to the Sydney Morning Herald.

*Essentially whoever stole the data was using a VPN.*

The ABC ran a story that an insider at Optus suggested it was [**human error**](https://www.abc.net.au/news/2022-09-23/optus-rejects-claim-hack-likely-result-of-human-error/101468846)and that an API was exposed to the internet with no security in place. Optus denied this claim.

*It was starting to appear at this stage that Optus had not been impacted by a highly sophisticated attack and had instead been impacted by an opportunistic cyber-criminal.*

There was confusion around which data breach this was, after a different user on BreachForums was offering 1.1million Optus customers data for sale on 17th September 2022. This data has now been removed from the forum and was unrelated to the Optus data breach. But it did cause confusion.

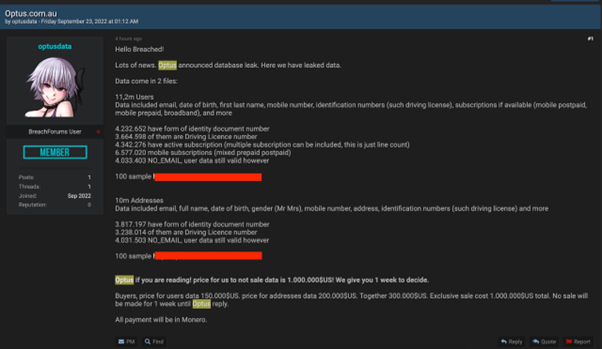


1.1 million Optus numbers — not related to the Optus Breach

Optus starting sending [**emails**](https://eftm.com/2022/09/finally-optus-begins-emailing-customers-after-massive-cyber-attack-227538) to impacted customers.

**Saturday 24 September 2022**

At around 3am AEST a user on BreachForums, ‘OptusData’ posted that they had stolen 11.2 million customers data from Optus via an exposed API. OptusData was demanding a $1millionUSD ransom in a week or they would start to sell the data.



‘OptusData’ the user who allegedly stole the Optus data post.

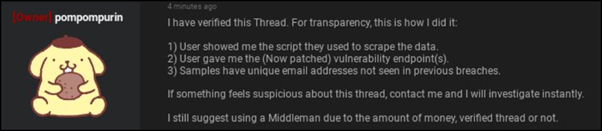
OptusData provided 2 sets of 100 lines of data as initial evidence, on review they appeared legitimate, several email addresses had no matches on [**Haveibeenpwned**](https://haveibeenpwned.com/) and several were ‘no\_email8230714@optus.com.au which is reportedly used by Optus as a filler if a customer does not provide an email.

Investigative Journalist [**Jeremy Kirk**](https://nam12.safelinks.protection.outlook.com/?url=https%3A%2F%2Ftwitter.com%2FJeremy_Kirk%2Fstatus%2F1573407117566152704&data=05%7C01%7C%7Cc572a84881604cac2e8c08daa07e1e51%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637998760824735156%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=nDQdg8APl7IaK7NLrb3VHUx3dd2igEsyynprOu%2FTNl8%3D&reserved=0) went to the effort of asking a neighbor who’s data was in the sample and they confirmed it accurate.

Jeremy Kirk then [**contacted**](https://nam12.safelinks.protection.outlook.com/?url=https%3A%2F%2Ftwitter.com%2FJeremy_Kirk%2Fstatus%2F1573652986437726208&data=05%7C01%7C%7Cc572a84881604cac2e8c08daa07e1e51%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637998760824735156%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=uFaZU%2B9s2G%2FKUejYeifw%2BR9P1I%2BQ%2F%2FMrSoifVYznGmk%3D&reserved=0)OptusData who confirmed they had gained access to the stolen data via an unauthenticated API: api.www[dot]http[:]//optus[.]com[.]au

*Optus reportedly shut this down, however they have not formally confirmed if this is the avenue of attack as of 28th September.*

The owner and administrator of BreachForums had also confirmed that the data stolen was legitimate and had ‘verified’ the post, meaning they were vouching for it being real.



Pom the owner and admin of BreachForums verifies the data.

*Some things were becoming clear at this point.*

*1, Optus was not attacked by a sophisticated actor, this is a threat actor who is conducting their business on an English Deep Web forum and does not have an alternative means of communication. They appear to be attempting a ransom negotiation in public. These all suggest they are not as sophisticated as Optus suggested.*

*2, The data stolen looked legitimate and had been verified by researchers and the owner of the forum, who was happy to put their credibility on the line.*

*3, Australia was about to hit a new level of panic around this data breach.*

The [**AFP**](https://nam12.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.abc.net.au%2Fnews%2F2022-09-24%2Fafp-monitoring-dark-web-for-stolen-optus-data-sold-online%2F101471256&data=05%7C01%7C%7Cc572a84881604cac2e8c08daa07e1e51%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637998760824735156%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=m8QgYOu1ikTO0oFGfdRNBRoTITpmBXsVsYCGHw%2B%2BzDM%3D&reserved=0) reported that they were monitoring the Dark Web for any Optus data that might be posted for sale according to the ABC.

Minister for [**Home Affairs**](https://nam12.safelinks.protection.outlook.com/?url=https%3A%2F%2Ftwitter.com%2FClareONeilMP%2Fstatus%2F1573559604457672705&data=05%7C01%7C%7Cc572a84881604cac2e8c08daa07e1e51%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637998760824891384%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=ZbK7vStB19sEl%2Bwtx1f6hDZW6ktbzHf158m3B3nmSD0%3D&reserved=0)Clair O’Neill posted a series of tweets about the unfolding situation.

**Sunday 25 September 2022**

The Department of Home Affairs announced they would introduce new [**security measures**](https://nam12.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.abc.net.au%2Fnews%2F2022-09-25%2Fnew-security-measures-to-be-unveiled-following-optus-data-breach%2F101472364&data=05%7C01%7C%7Cc572a84881604cac2e8c08daa07e1e51%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637998760824891384%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=8GvVlimzTreYGmAy8E1EEbymyX5tliK3zvUnWQXfPWA%3D&reserved=0) after the Optus breach. Reportedly the new measures would address reporting times of breaches.

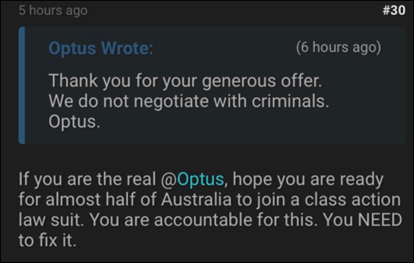
Shadow Government Services Minister Paul Fletcher stated that Optus [**did the right thing**](https://www.skynews.com.au/opinion/optus-did-the-right-thing-coming-out-quickly-on-breach-of-information/video/6c451c1e7ef83b4b943ac2c266b409db) “coming out quickly” and advising Australians on the breach of their information.

**Monday 26 September 2022**

Prime Minister Albanese commented on the breach, calling it a [‘**huge wake up call’.**](https://nam12.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.facebook.com%2F9News%2Fvideos%2Foptus-cyber-attack-a-huge-wake-up-call%2F484799193315282%2F&data=05%7C01%7C%7Cc572a84881604cac2e8c08daa07e1e51%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637998760824891384%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=vziZt6jTKnUOeGkWQijFGMariR2bhNhr%2BUX91F9zM%2BU%3D&reserved=0)

An executive from Optus held a radio interview with 2GB and claimed that Optus had not [**reviewed**](https://nam12.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.2gb.com%2Foptus-struggles-to-explain-their-data-breach-in-trainwreck-interview%2F&data=05%7C01%7C%7Cc572a84881604cac2e8c08daa07e1e51%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637998760824891384%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=VBjtRlFU4cpqMzqea9O%2Fgd7DN0QkC91cbSqVj2tYI3g%3D&reserved=0)the alleged breach data on the forum.

A new user on BreachForums calling themselves [**‘Optus’**](https://nam12.safelinks.protection.outlook.com/?url=https%3A%2F%2Ftwitter.com%2FCyberknow20%2Fstatus%2F1574102591834685440&data=05%7C01%7C%7Cc572a84881604cac2e8c08daa07e1e51%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637998760824891384%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=hygIgyYe3fygAzeiuUMQYIwS%2BToayz8d7wQTFXFuG38%3D&reserved=0) posted to the thread of OptusData to decline the $1millionUSD ransom stating they ‘don’t negotiate with criminals’. This was not Optus but did frustrate OptusData.



Fake Optus account on BreachForums enrages OptusData

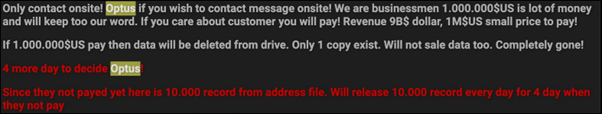
BreachForums was also being flooded with new users who were only adding extra pressure to the situation.

The Minister of Home Affairs declared that the attack was [**not sophisticated**](https://www.abc.net.au/radionational/programs/breakfast/optus-breach-politics-with-david-crowe/101476592)**.**

Optus announced they would be offering [**free credit monitoring**](https://7news.com.au/technology/optus/optus-to-offer-credit-monitoring-program-amid-fears-data-breach-could-lead-to-identity-theft-c-8360053) from Equifax to most high-risk customers.

**Tuesday 27 September 2022**

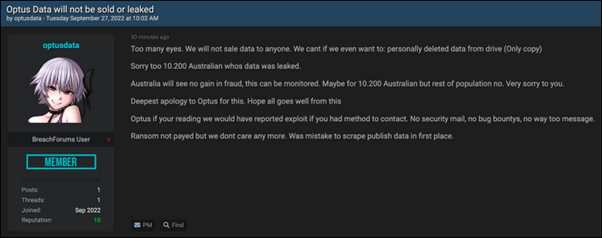
OptusData released 10,000 additional users’ data and threatened Optus to pay the ransom, or they would post 10,000 further customers for 5 more days.



OptusData leaks 10,000 more records and demands ransom payment.

[**Jeremy Kirk**](https://twitter.com/Jeremy_Kirk/status/1574498097194901504) reviewed the data and discovered that there were also Medicare numbers present.

Four hours after OptusData posted 10,000 customers data they announced they had deleted the entire data-set and were ending the ransom, they also apologized.



OptusData declares they have deleted data and are stopping the extortion.

*It is unclear exactly why this has taken place, it is possible that OptusData sold the data-set, or they may have been spooked by the interest of law enforcement, their activities and interactions suggested they may have had poor opsec and could be trying to cover their tracks.*

*However, this is a highly valuable data-set, and they would have no doubt been offered good money for it. It is safe to assume that the entire data-set is still out in the wild and that precautions should be taken accordingly.*

Jeremy Kirk did confirm that Optus had told him they [**did not pay**](https://twitter.com/Jeremy_Kirk/status/1574599963987714050) a ransom for the data.

Text

Description automatically generated

Jeremy Kirk gets confirmation from Optus.

For a comprehensive wrap up of this sequence of events Jeremy Kirk put together an article for [**bankinfosecurity**](https://www.bankinfosecurity.com/optus-attacker-halts-au15-million-extortion-attempt-a-20157) which is well worth reading.

Unfortunately, other users on BreachForums had already obtained the 10,000 files and reposted them to the forum, regardless of what has happened to the rest of the data the users in this data-set are at highest risk.



A different user on the forum re-posts the leaked 10,200 Optus customer files

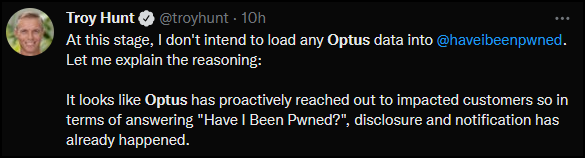
There are reports that a [**class action**](https://www.sydneycriminallawyers.com.au/blog/class-action-could-be-launched-against-optus-over-data-breach/)could be launched against Optus.

Optus customers have received a poor attempt at [**extortion**](https://7news.com.au/technology/optus/cyber-criminals-using-optus-hack-to-target-anxious-australian-customers-with-new-scams-c-8371154)via text message using the current Optus breach as a lure.

The Australian government has reportedly asked the [**FBI**](https://www.theguardian.com/australia-news/2022/sep/27/federal-government-under-pressure-to-reveal-optus-data-breach-plan-as-fbi-called-in-to-help) for assistance.

Australian states are providing guidelines for impacted Optus customers on how to [**change their license numbers**](https://www.sbs.com.au/news/article/optus-data-breach-how-you-can-get-a-free-replacement-drivers-licence/1ifnlrd2p)**,** with Optus planning to reimburse them for costs.

[**Troy Hunt**](https://twitter.com/troyhunt/status/1574582128385224705) who owns and runs Haveibeenpwned confirmed that he would not be adding the currently exposed 10,200 customers data due to notification already taking place.



Troy Hunt declares he will not be uploading the stolen data to HIBP

*There has been a noticeable uptick in additional Australian data for sale or on offer on BreachForums since the media attention of the Optus breach. Noticeably on Tuesday night there was a school data, old Telstra and NAB data along with over with a 2 million user/password list posted.*

*Australia is now well and truly front of mind for cyber criminals and all Australian organizations and citizens can expect an increase in cyber-criminal activity for coming weeks.*