Australian charged for ‘Evil Twin’ WiFi attack on plane

By Bill Toulas

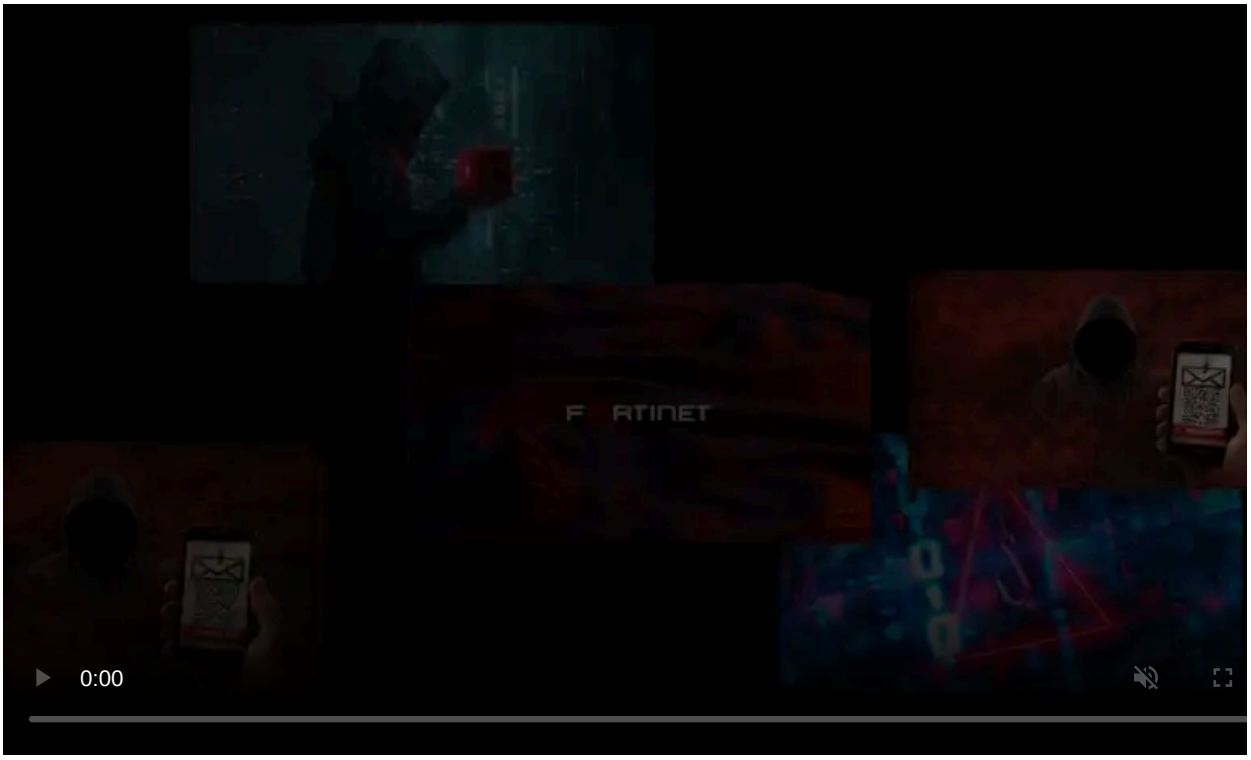
Published: 2024-07-01 · Archived: 2026-04-06 01:38:27 UTC

An Australian man was charged by Australia's Federal Police (AFP) for allegedly conducting an 'evil twin' WiFi attack on various domestic flights and airports in Perth, Melbourne, and Adelaide to steal other people's email or social media credentials.

The police started investigating reports from airline employees in April 2024 and found evidence of the man performing malicious activities after examining his devices seized at the airport.

Evil Twin WiFi attack

An evil twin WiFi network is a malicious/fake wireless access point that uses the identical SSID (WiFI network name) as that of a legitimate or expected network in a specific area. For example, many flights offer in-flight WiFi, requiring passengers to first connect to the airline's WiFi network.


F RTINET
0:00

When a cybercriminal conducts an evil twin attack, they set up a WiFi network under their own control that uses the same name as the one promoted by the airline.

However, users attempting to connect to the malicious access points are directed to a fake login page or a captive portal webpage, asking them to log in using email addresses, passwords, or other credentials.

In the case of the Australian arrested by AFP, the agency says that he used a portable device to create free WiFi access points at multiple locations, requiring them to log in using their email or social media accounts.

The man collected this information, which could be later used to access more sensitive data, hijack social media accounts, extort victims, or sell it to other cybercriminals.

"AFP cybercrime investigators have allegedly identified data relating to the use of the fraudulent WiFi pages at airports in Perth, Melbourne and Adelaide, on domestic flights and at locations linked to the man's previous employment," explains the AFP.

Investigation into the post-exploitation activity and the extent of the man's operation is still underway.

The criminal charges the suspect faces are:

1. Unauthorized impairment of electronic communication, incurring a maximum penalty of 10 years in prison.
2. Possession of control of data with intent to commit a serious offense, incurring a maximum penalty of 3 years in prison.
3. Unauthorized access or modification of restricted data, incurring a maximum penalty of 2 years in prison.
4. Dishonestly obtaining or dealing in personal financial information, incurring a maximum penalty of 5 years in prison.
5. Possession of identification information with intent to commit an offense, incurring a maximum penalty of 3 years in prison.

Malicious or untrustworthy WiFi access points are always possible in public spaces, so people who need to use them should be careful about sharing their other login credentials when attempting to use them.

It is also advised to turn off file sharing on untrusted WiFi networks and use a VPN to encrypt internet traffic and prevent the capture of sensitive information.

Not a common attack

While it is not unheard of for threat actors to conduct these types of WiFi attacks, cybersecurity researcher Daniel Card warns that evil twin attacks are not something most people need to worry about.

"This kind of attack is totally possible, as we do it in labs and as part of security testing/training but it's rarely seen in the wild," Card told BleepingComputer.

"It's close proximity phishing. Out of all the incidents myself and friends deal with I've never seen or heard about this in the wild other than when used by GRU (or at hacker conferences as a demo/joke/ctf). Outside of GRU (who also got caught), I only have heard of one other case."

The researcher is referring to the 2018 indictments of Russian state-sponsored GRU hackers who conducted evil twin attacks to monitor targets' internet traffic.

Card says that telling people not to use WiFi is unrealistic, as the need to remain online, especially on long trips, has become crucial for employees and students.

Instead, Card says that usernames and passwords are flawed authentication mechanisms, which is why MFA and robust security standards are necessary to protect our accounts.
