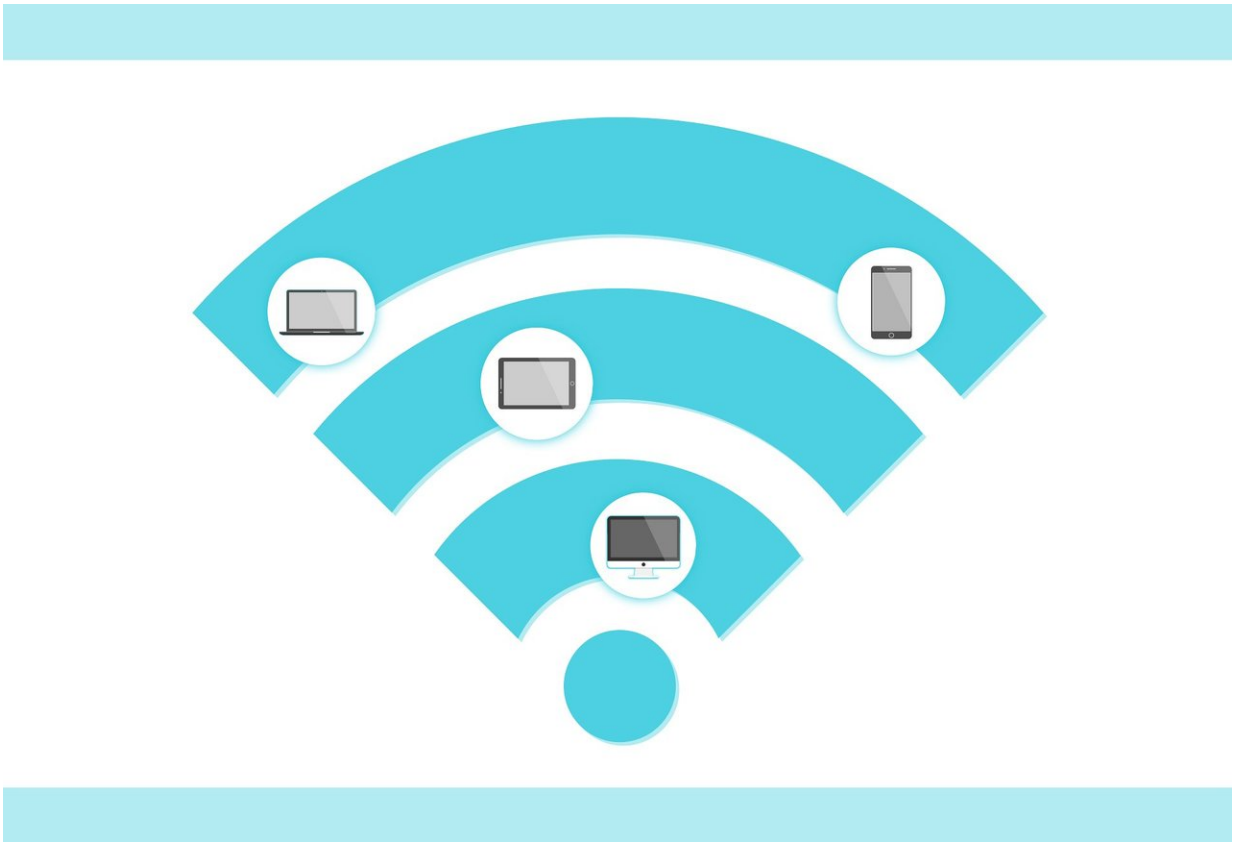
Security researcher discovers hotspot finder app with leaks

April 23 2019, by Nancy Cohen



Credit: CC0 Public Domain

Another day, another app mishap story, and it is in the Ouch range. This one is called WiFi Finder.

From the app's Privacy Policy page: "Proofusion built the WiFi Finder app as a Free app. This SERVICE is provided by Proofusion at no cost and is intended for use as is."

Brandon Hill, *HotHardware*, explained that the idea of using such an app would be to make it easier for you to locate free public Wi-Fi hotspots for use on-the-go.

A security researcher discovered that it wasn't just collecting public network information. It was collecting data from private WiFi networks in residential areas.

TechCrunch had the details.

While the developer claimed the app only provided passwords for public hotspots, "a review of the data showed countless home Wi-Fi networks. The exposed data didn't include contact information for any of the Wi-Fi network owners, but the geolocation of each Wi-Fi network correlated on a map often included networks in wholly residential areas or where no discernible businesses exist."

The hotspot finder app for Android leaked 2 million Wi-Fi network passwords, said reports on Monday. Repeat for emphasis. Wi-Fi network passwords, *2 million*.

The passwords were discovered in the database. *TechCrunch* said, "Tens of thousands of the exposed Wi-Fi passwords are for networks based in the U.S."

According to the Google Play listing for WiFi Finder, "This application can connect the device to WiFi networks with legit credentials. Always use the safe networks. Connect to hotspots for internet access! You can use WiFi Finder to connect to Wi-Fi hotspots."

TechCrunch said, "The app allows the user to upload Wi-Fi network passwords from their devices to its database for others to use." With the database of those many network passwords left exposed, it was allowing anyone to access and download contents in bulk.

Brandon Hill, *HotHardware*, said private SSID and password credentials were accessible, and also "the precise geolocation of the routers in question." *Gizmodo* said downloading WiFi Finder, for example, required users to surrender access to their locations, contact lists.

Hill's further observation: "With geolocation data of home networks, passwords and SSID information, it would be trivial for attackers to use this information to gain unauthorized access."

Now, what?

TechCrunch was highlighted by other reports and widely quoted regarding this WiFi Finder incident, reported by Zach Whittaker: "We spent more than two weeks trying to contact the developer, believed to be based in China, to no avail. Eventually we contacted the host, DigitalOcean, which took down the database within a day of reaching out."

At the time of this writing the rating on Google Play was 3.8.

One review on the Google Play page was dated April 23, 2019, saying this app leaked 2 million wifi passwords in plaintext.

Observation from *Gizmodo*: "Hypothetically, an attacker could use the credentials to fiddle with router settings, intercept logins, spread malware across a network, and takeover smart home devices, such as security cameras. Career cybercriminals would likely find this process tedious, however."