

The WiFi Coconut is a router's evil twin

Wi-Fi is how most people connect to the internet most of the time – but from a security standpoint, it's a remarkably wobbly foundation.

We treat Wi-Fi connections like hardened tunnels to wherever we're connecting on the internet, but there's nothing inherently private about the signal. Wi-Fi is just radio, and like any radio, the signals go out in all directions all the time. Anyone with the right antenna can listen to what's being broadcast, and it's nearly impossible to tell that they're doing it. Even more dangerous, anyone can offer Wi-Fi, so it's hard to be absolutely sure who you're connecting to. This is why hardened systems like SecureDrop often pull out a computer's Wi-Fi card completely. Without wireless capability, the attack surface of a device shrinks dramatically.

Actually exploiting those weaknesses is difficult, but it's far from impossible... which is where devices like the WiFi Coconut come in.

a: hover]: shadow-highlight-franklin
[&>a]: shadow-underline-black
dark: [&>a: hover]: shadow-highlight-
franklin **dark: [&>a]: shadow-**
underline-white **md: text-40** **lg: -**

ml-100">What can it do?

The biggest threat is something called a KARMA attack in which attackers disguise themselves as a trusted Wi-Fi network. If you've ever been told to avoid open Wi-Fi networks in public places, this attack is the reason why – although surprisingly, it works even if you're nowhere near an unsecured network.

The attack exploits the peculiar way computers connect with preferred Wi-Fi networks. When you set your computer to automatically connect, it starts proactively looking for that network, sending requests that also identify what network it's looking for. As this post memorably put it, it's as if your device is constantly shouting, "Is Starbucks WiFi here?" And unlike most Wi-Fi traffic, those signals are unencrypted.

In the KARMA attack, the attacker uses a device like the WiFi Coconut to pick up on those signals and give whatever answer your device is looking for. It will send back a message identifying itself as whatever you're looking for, like Starbucks Wi-Fi, and invite your device to automatically join the network. Because of the seamless way devices switch between Wi-Fi networks, there's a good chance it will happen without you even noticing. Suddenly, you're connecting to the internet through someone else's router, exposing you to all manner of malware injection attacks.