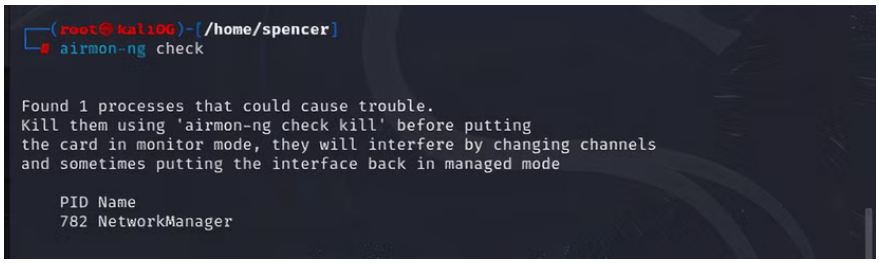
What can hackers actually do if they gain access to your Wi-Fi router?

Whether hackers target your router to satisfy their curiosity or have actual malicious intentions, here's everything they can do if they have access to this networking device.

Your Wi-Fi router manages network traffic and acts as your gateway to the Internet, but what happens if it falls into the wrong hands? Whether hackers are targeting your router out of curiosity or have actual malicious intent, here's everything they could do if they gain access to this networking device.

Note : Please note that while all of these issues are real, an attacker needs to have access to your router in order to be successful.

Prevents you from accessing the router



Being kicked off your home network repeatedly can be extremely annoying, but that's what some hackers do. Hackers can use a deauthentication attack to target network devices. To do this, hackers don't even need admin access to your router; they just need to find the router and the device you're using. They can do this using a tool like Aircrack-ng. Once they do, they create a command that takes advantage of the router's authentication protocol to deauthenticate, thus kicking you off the network.

If they access the router using the default admin credentials, which are available online, then disabling your Wi-Fi is much easier. Once they log into the router's portal using these credentials, all they need to do is find the MAC address associated with the device and blacklist it.

Change admin login and SSID

A study by Forbes found that 86% of users never change their default login credentials. Since default login credentials are easily found online, all a hacker will do is do a quick Google search to find the information they need and log into your router. If successful, they can change things like the password and SSID. Changing the

password will kick you off the network, and changing the SSID will change the name of your network.

They can also completely hide your network after kicking you out and renaming you, making it difficult to get you back online.

Turn your router into a bot and redirect traffic

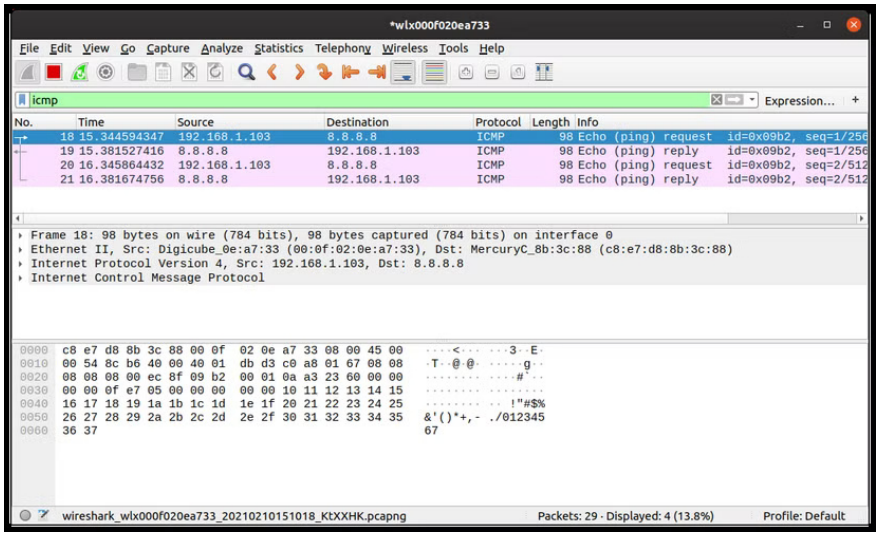
A botnet is a network of infected computers under the control of a botnet herder. After infecting your router with malware, hackers can integrate it into a botnet and use it to carry out DDOS attacks or send mass spam.

Imagine for a moment that your router is part of a botnet. It is now one of thousands of infected devices, all controlled by a single individual. Criminals often use botnets to launch distributed denial of service (DDOS) attacks. These attacks aim to overload a server with traffic until it is no longer available.

Hackers can use your router as part of a DDOS attack through a DNS hijacking attack. This attack is performed by changing the router's DNS settings to redirect all incoming traffic to a specified IP address.

Hackers can also redirect traffic to malicious websites that steal sensitive information or infect your computer with malware.

Stealing sensitive information



If configured correctly, your router will use a secure encryption standard like WPA2 or WPA3. But if hackers gain control of your router, they can downgrade or even remove the encryption.

Without encryption, data is sent in plain text. If this plain text data is intercepted, attackers can easily extract sensitive information such as login credentials that can be used to access your most important accounts.

Now, it should be said that introducing HTTPS as a standard for most websites helps solve this problem, but you still don't want someone spying on your network.

Install malware on router

Once they gain access to your router, hackers can download malware to take control of the router and the data running through it with ease.

In 2016, the VPNFilter malware infected millions of routers. VPNFilter was created to steal personal information and integrate hacked devices into botnets. The malware automates operations that would otherwise be performed manually by hackers, making it easier to control the infected network and the devices on it.

And remember those botnets we talked about earlier? Same problem.

Luckily, there are a few easy ways to keep your router secure: Change the default login information and keep your Wi-Fi router up to date. Just those two small changes will make it much harder for someone to gain access to your router, and you'll keep your network much more secure by doing so.

If you live in a crowded area, consider ways to keep your Wi-Fi safe from nosy neighbors!