SENRIO

Lateral Movement

IoT Hopscotch: Hacking a Network Without Touching a PC

ID Camera

STEP 1

This Axis security camera was vulnerable to the Devil's Ivy vulnerability, and accessible via the public Internet. Exploiting it gives us custom code execution and access to its feed.

Exploit Camera

STEP 2

Through the camera feed, we can see an office worker input their username and password to a Network Attached Storage device.

Find Router

STEP 3

Interrogating the router allows us to determine if its vulnerable to a known exploit, giving us admin ID and password.

Compromise Router

STEP 4

The router runs a service that accepts remote commands on a UDP port and contains a stack overflow vulnerability, which we exploit, gaining code execution.

Change Rules

STEP 5

We use our low-level control of the router to change network rules that prevented the camera from communicating with the NAS.

Access NAS

STEP 6

We are able to log into the NAS from outside the target network via the camera and router. We can now exfiltrate files from the NAS.

Why Should You Care?

The impact of a security vulnerability on an IoT device may not be limited to just that device. If you lack awareness of and visibility into what ALL your connected devices are doing, you cannot effectively detect and respond to threats. If this had been your enterprise, would your end-point and network defenses have caught this type of attack? If not, or only with difficulty and not before exfiltration, let's talk about how we can remedy that situation.

http://iot.security