How to Detect Killer Cables from Hacker Space

by Kevin D. Murray, CPP, CISM, CFE

They Appear Normal
They Blend In
They Suck Up Your Data

They are the Killer Cables from Hacker Space.

Imagine a charging cable which looks exactly, and I mean ***exactly***, like any stock charging cable. Oh, just one difference. This charging cable has built-in Wi-Fi and can run penetration programs on whatever it is plugged into.

It exists, in four versions and two colors, white and black, and sells for $119.99.

Ostensibly, "is built for covert field-use by Red Teams." However, anyone can buy one. We did, to determine if the following claims were true.

- "It looks like the real thing. It feels like the real thing, down to the millimeter."
- Has "features that enhance remote execution, stealth, and forensics evasion."

Our tests revealed it lives up to its claims.

Basically, this is a malicious wireless implant for computers. It's a rigged USB cable that allows remote attackers to attack via Wi-Fi.

When plugged into a computer the operating system detects the cable as a Human Interface Device (HID), for example a keyboard.

The cable can broadcast its own Wi-Fi SSID acting as an access point, or it can be preconfigured to connect to a predetermined

Wi-Fi network and act as a client, meaning it can use your network to hop on the internet.

Connecting to a predetermined network makes the cable even more difficult to detect. And, it may allow an attacker to open up a reverse shell to a remote computer where the attacker can issue commands. Simply speaking, the remote hacker has full access to your device.

Has your charging cable been switched?
Have you thought to check? Probably not.

How to Detect Killer Cables from Hacker Space

by Kevin D. Murray, CPP, CISM, CFE

How to Identify an Alien Cable?

Our TSCM team worked on the problem…

The cable's Wi-Fi signal is stealthy, but it can be detected. If you know what characteristics to look for, wide areas of offices space can be scanned quickly.

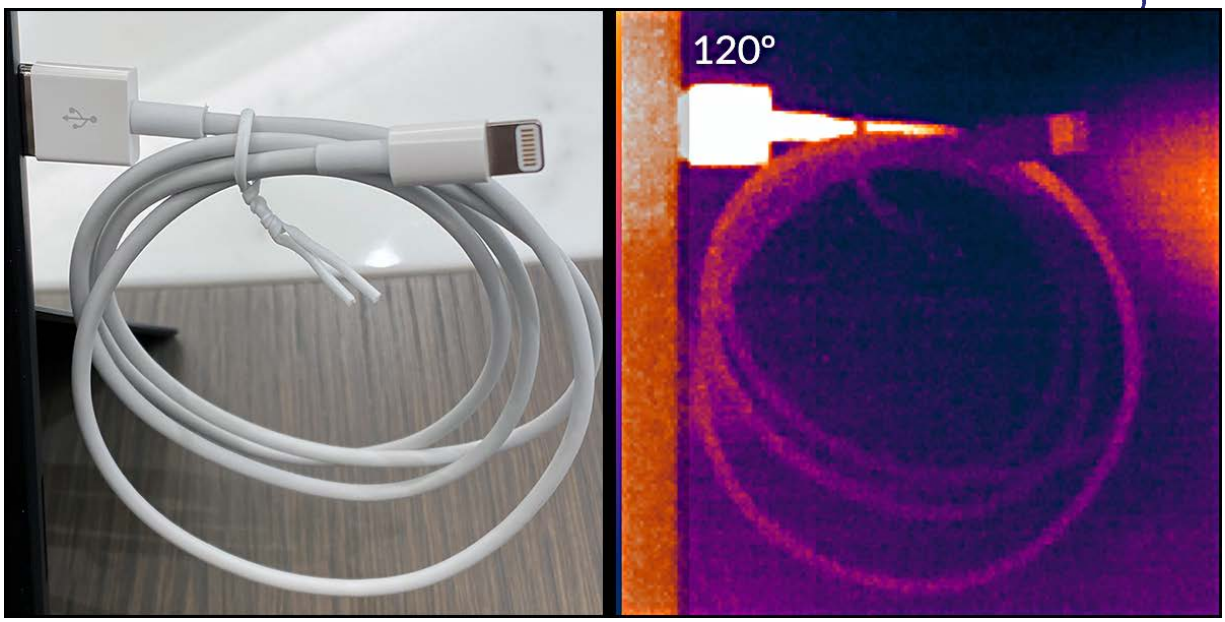
As in **War of the World's**, the invader has an **Achilles heel**. Electronic circuits generate heat. This Martian is no different. When plugged in and operating the USB-A[1] side of the cable measures between 115º and 125º Fahrenheit.

Prevention Tips

- Check Apple's guide to fake cables.[2]
- Mark *your* cables with an indelible pen.
- Use a USB wall charger instead of a computer.
- Conduct TSCM inspections which include your Wi-Fi. In addition to finding killer cables, inspections find other rogue devices as well.

If you have any questions, or would like to schedule home office TSCM / information security audits, just let me know.

Kevin



Although an infrared camera can identify these aliens you don't need **Men in Black** capabilities like this. Just touch the plug. If it feels warm you've got big problems, and you should call us.

Kevin D. Murray CPP, CISM, CFE is a business counterespionage consultant and TSCM specialist with over four decades of experience.

Murray Associates[3] is an independent security consulting firm, providing eavesdropping detection and counterespionage services to business, government and at-risk individuals. Headquartered in the New York metropolitan area, a Murray Associates team can assist you quickly, anywhere in the United States, and internationally.

[1] https://en.wikipedia.org/wiki/USB_hardware

[2] https://support.apple.com/en-us/HT204566

[3] https://counterespionage.com/about-murray-associates/electronic-eavesdropping-detection/