This iPhone charging cable can hijack your computer

By Zack Whittaker

Published: 2019-08-12 · Archived: 2026-04-05 16:55:50 UTC

Most people don't think twice about picking up a phone charging cable and plugging it in. But one hacker's project wants to change that and raise awareness of the dangers of potentially malicious charging cables.

A hacker who goes by the online handle MG took an innocent-looking Apple USB Lightning cable and rigged it with a small Wi-Fi-enabled implant, which, when plugged into a computer, lets a nearby hacker run commands as if they were sitting in front of the screen.

Dubbed the O.MG cable, it looks and works almost indistinguishably from an iPhone charging cable. But all an attacker has to do is swap out the legitimate cable for the malicious cable and wait until a target plugs it into their computer. From a nearby device and within Wi-Fi range (or attached to a nearby Wi-Fi network), an attacker can wirelessly transmit malicious payloads on the computer, either from pre-set commands or an attacker's own code.

Once plugged in, an attacker can remotely control the affected computer to send realistic-looking phishing pages to a victim's screen, or remotely lock a computer screen to collect the user's password when they log back in.

MG focused his first attempt on an Apple Lightning cable, but the implant can be used in almost any cable and against most target computers.

"This specific Lightning cable allows for cross-platform attack payloads, and the implant I have created is easily adapted to other USB cable types," MG said. "Apple just happens to be the most difficult to implant, so it was a good proof of capabilities."

In his day job as a red teamer at Verizon Media (which owns TechCrunch), he develops innovative hacking methods and techniques to identify and fix security vulnerabilities before malicious attackers find them. Although a personal project, MG said his malicious cable can help red teamers think about defending against different kinds of threats.

"Suddenly we now have victim-deployed hardware that may not be noticed for much longer periods of time," he explained. "This changes how you think about defense tactics. We have seen that the NSA has had similar capabilities for over a decade, but it isn't really in most people's threat models because it isn't seen as common enough."

"Most people know not to plug in random flash drives these days, but they aren't expecting a cable to be a threat," he said. "So this helps drive home education that goes deeper."

MG spent thousands of dollars of his own money and countless hours working on his project. Each cable took him about four hours to assemble. He also worked with several other hackers to write some of the code and develop exploits, and gave away his supply of hand-built cables to Def Con attendees with a plan to sell them online in the near future, he said.

But the O.MG cable isn't done yet. MG said he's working with others to improve the cable's functionality and expand its feature set.

"It really just comes down to time and resources at this point. I have a huge list in my head that needs to become reality," he said.

(via Motherboard)

Zack Whittaker is the security editor at TechCrunch. He also authors the weekly cybersecurity newsletter, this week in security.

He can be reached via encrypted message at zackwhittaker.1337 on Signal. You can also contact him by email, or to verify outreach, at zack.whittaker@techcrunch.com.

View Bio ›
