Why you should really, really update your Logitech wireless dongle

Three and a half years ago, a security researcher broke into my laptop without ever needing to touch it. He didn't even need its network address. All he had to do was sniff out my Logitech wireless mouse's tiny USB receiver, fire off a few lines of code, and start typing things *that appeared on my screen*. He could have wiped my hard drive, installed malware, or worse, much as if he'd had physical access to my PC.

Practically any Logitech wireless mouse and keyboard was vulnerable to the issue, they said. It was the kind of hack I'd laugh at in a terrible hacker movie — the kind that seems too convenient* to actually exist.

But when I wrote about the so-called "MouseJack" hack in 2016, I figured that was that. I'd given the issue attention in a major technology news publication, lots of people were reading about it, and Logitech had already issued a patch.

Yet I'm now learning that the world may not be rid of MouseJack yet.

Earlier this week, security researcher Marcus Mengs revealed that Logitech's wireless Unifying dongles are actually vulnerable to a variety of newly discovered hacks as well, primarily ones that are paired with presentation clickers, or during a brief window of opportunity when you're pairing a new mouse or keyboard to the dongle. I didn't think much of that last one — Logitech's peripherals come pre-paired, and you'd have to be a pretty lucky hacker to know exactly when someone

has lost their dongle (or mouse) and is setting up a new one.

Something else in Meng's report (and *ZDNet*'s coverage) caught my eye, however – an allegation that Logitech is *still* selling USB dongles vulnerable to the *original* MouseJack hack.

I got in touch with Marc Newlin, the Bastille researcher who originally hacked me in 2016, and he immediately corroborated the report: He'd just recently purchased a Logitech M510 mouse that still came with a vulnerable dongle as well.

So I spoke to Logitech, and a rep admitted that those unpatched dongles may still be on the market. In fact, Logitech says never actually recalled any products after the original hack in 2016:

> *Logitech evaluated the risk to businesses and to consumers, and did not initiate a recall of products or components already in the market and supply chain. We made the firmware update available to any customers that were particularly concerned, and implemented changes in products produced later.*

Logitech it did "phase the fix in" for newly manufactured products, but a rep said they can't yet confirm when the changes were made at the factory.

Not that we should necessarily be singling out Logitech, mind you. According to Newlin, MouseJack affected devices from Dell, HP, Lenovo and Microsoft too, and possibly others that used the same Nordic and Texas Instruments chips and firmware for their wireless receivers. Since Logitech lets you update the firmware on its Unifying dongles, they were better off than most.

But that's also why Logitech's dongles could be a cheap and easy way to launch the attack to begin with – in 2016, Newlin showed me that the Logitech Unifying Receiver itself can be

used as a radio to sniff out and hack other dongles, even though he says has far better range.

All of this is to say that if you've got a wireless Logitech mouse, keyboard, or presentation clicker, you should probably patch it now — and maybe again in August when Logitech will be rolling some additional fixes out. Logitech's old support pages for MouseJack are gone, but here's the link to update any Unifying receiver, and if you have a G900 gaming mouse.

That's Logitech's recommendation too: "[A]s a best practice, we always recommend people update their wireless Unifying USB receivers to our latest firmware."

**I was pretty skeptical in 2016. That's why I provided my own laptop and my own Logitech dongle for Bastille to demo it for me.*

https://www.theverge.com/2019/7/14/20692471/logitech-mousejack-wireless-usb-receiver-vulnerable-hack-hijack