The Dirty Truth About USBs

By Joseph Regan on February 21, 2020

Did you know there's one fool-proof exploit hackers can take advantage of to snag your data? It's a vulnerability every system has, from PCs to Macs to mobile devices. And what's worse, there's no antivirus in the world that can cover it, nor a patch that can fix it. Cybersecurity professionals are baffled by it, yet remain powerless to address it.

What is this nefarious, dangerous exploit?

It's you, of course!

As cybersecurity grows more advanced and powerful, many hackers are finding it harder to find weaknesses in the actual software side of things. Which is why they've been increasingly reliant on taking advantage of human error to reach your most valuable data. Phishing emails will try to exploit fear, malware hidden on torrent sites could be using greed, and other scammers may try to weaponize your compassion — or even your loneliness — against you.

But for the humble USB drive, the most reliable exploit hackers have is our curiosity.

Curious about curiosity

According to astrophysicist and author Mario Livio, there are two basic types of curiosity: perceptual curiosity, which is when you learn something surprising (and often unpleasant) and gives you an itch you need to scratch, and epistemic curiosity, which is when you want to learn something because you think it will be pleasurable and you anticipate an award. Both have been vital in our biological — and technological — evolution.

So you might feel perceptual curiosity if you read a terrifying headline on a news site about the latest natural disaster. It may not make you "happy", but it would bother you all day if you didn't investigate further. On the other hand, you'd probably feel epistemic curiosity if you got an email from a friend with a text document labeled "LOVE-LETTER-FOR-YOU" attached to it — especially if that friend is pretty cute.

Which is exactly how the ILOVEYOU virus spread back in 2000, doing an estimated $5.5–8.7 billion in damages worldwide.

That's far from an isolated case. From pop-ups saying you won an online sweepstakes to strangers on social media claiming they're old friends from high school, hackers have been using epidemic curiosity to trick people into clicking links and downloading files for as long as there's been email. In fact, some of the most successful virus delivery methods are just empty emails with links or files — people are so curious they just straight-up download them, making the hacker's job a million times easier.

Hackers are so good at weaponizing curiosity that they've even used it to pull off some of the biggest hacks of the decade.

Which is what brings us back to the USB stick.

USB - the Ultimate Security Breach

What would you do if you found a USB — which actually means Universal Serial Bus, and is sometimes called a thumb drive — device on the ground?

If you're like most people, you'd probably be curious — especially if the device had an especially tantalizing label, something like "confidential", or "porn", or "do not open". In which case, the next time you get to a PC (either at work or at home, depending on the label), you might plug it in. You could do it altruistically, hoping that the information it contains could help you find its owner — or maybe voyeuristically, just to see what's inside. But in the very likely case the USB was planted by a hacker, your motivations won't matter one bit: they'll be well on their way to infecting your device.

There are two ways that a USB device could deliver its payload. The first way is treating them just like emails: they have an infected file saved on them, and it's up to you to click and run the file in order for the infection to reach your computer. In this case, you could plug the device into your PC or Mac and scan it for viruses before you open anything inside, which would be the second-most cautious thing you could do… other than not plugging it in at all.

But the problem with USB devices is that most of the time, their manufacturers don't protect their firmware — which means clever hackers can reprogram them to be more efficient and dangerous. The most common way to do that is to reprogram the USB device to automatically upload malware onto any device it's plugged into, even before you open it. In this case, the moment you plug the device in, you're at risk.

"I'm in"

But if you think hackers can only use USB devices to deliver malware, you're sadly mistaken. These techno-wizards have devised, by last count, up to 29 different ways to use USB drives to do different things to your device and your data.

For example, a USB attack could:

- Take over your keyboard and enter predetermined keystrokes, forcing your PC to perform actions you wouldn't want
- Log your keystrokes and send the data to remote servers
- Implant hardware, such as a radio receiver
- Change or manipulate your files
- Infiltrate your webcam and record you
- Broadcast your activity on publicly accessible electromagnetic emissions
- Permanently destroy your device with a powerful electrical surge

And that's just a few examples in a growing list that becomes more impressive — and frightening — as we develop new USB devices and software. But you may be thinking: just because it's *possible* doesn't mean it's *likely*, right? Is there really a hacker out there hiding dangerous USB devices like some kind of criminal Easter Bunny?

You'd be surprised.

Charging into danger

You've just landed at LAX in 2019, and you're exhausted. You're thirsty, your legs are sore, and worse of all, your smartphone is almost dead. Fortunately, LAX has free phone charging stations, so you plug your smartphone into one for a bit to get some much-needed juice before the final leg of your journey.

And when you finally turn it on and check your phone, woops, that USB charging station was hacked and now your phone is infected.

Another example: you go to work one day, and on the way, sitting on a bench, you see a USB device. You pick it up, maybe thinking it's a co-worker's, but when you plug it in, you get a big, fat message that says you just failed a cybersecurity test — which may be the best-case scenario in that situation.

Because not only do these things happen, they work really well when they do. While there are no solid numbers of how many "USB Drop Attacks" happen per year, a 2016 study showed that, of 297 infected USB devices dropped around a university campus, 98% were found, and 45% were plugged into a PC. That's almost a 50% success rate — compared to the estimated .5% of people who fall for phishing emails (the most popular attack vector today). That's huge.

So while the odds of a hacker dropping a USB device in your driveway might be pretty low, if you work at a big company or for the government, watch out: you're probably way more likely to run into a random USB device laying on the ground than the rest of us.

Stay unplugged, stay safe

So this begs the question: how do you stay safe from infected USB devices?

Well, that’s simple — don’t plug in USB devices you find lying around. If you find one outside of your business, take it to IT or tell your boss about it. Chances are there are more than one and it’s possible not all your co-workers are as technically savvy as you. If you find one in a public place, do the world a favor and throw it out, either to protect yourself and strangers from malware, or to make sure whoever lost it doesn’t have their private information violated by someone they don’t know. And if you must charge your phone in public, only use AC chargers — anything else could be risky.

Curiosity can lead us to discover some amazing things — but don’t let it become your biggest cybersecurity downfall!