This unremarkable looking Lightning cable can steal your data and send it to hackers

Apple has switched to using the USB-C connection standard on the latest generation of iPad Pro, and this should probably be applied to new iPhone models soon as well. This not only provides convenience, but also helps limit security risks.

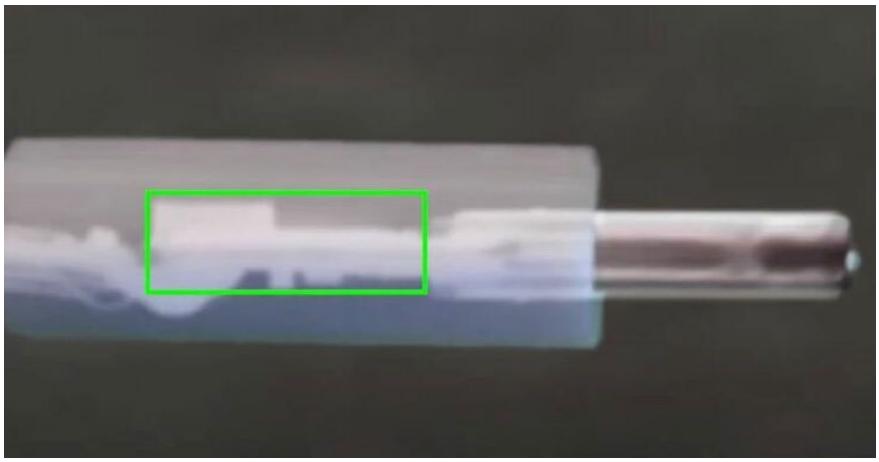
The reason for saying that is because an international security researcher has recently successfully developed a Lightning cable that looks quite ordinary, or rather, is no different from a Lightning cable that comes with the iPhone, but it is not. possess the ability to steal passwords and remote kernel data from any target. The stolen data will then be sent to the hacker without the victim's knowledge.

This dangerous cable is called OMG, and it basically works like a normal Lightning cable. That is, it still supports users to charge the battery and transfer data, only there will be one more unwanted malicious 'feature', which is stealing data from the connected system.

Vice's report shows that it is difficult for users to detect the difference between this malicious OMG cable and Apple's regular Lightning, because they have too similar external designs. However, the real difference will lie on the inside, when the OMG cable is integrated with a rather complex chip system, which can record keystrokes as well as clicks and touches on the user's screen when connected. connects to MacBooks, iPads, and even iPhones. It then sends back data about a malicious agent that can live for miles away. This involves creating a WiFi hotspot that hackers can access, and then using the necessary tricks to steal data from the target device. For example, hackers can embed keylog software in the cable, which can continuously collect keystroke data of the target in real time.

And yet, this malicious Lightning cable also includes a geolocation feature that, when activated, can act as a blocker to the device's payload according to its location. This will help prevent accidental leakage of keystrokes from other devices. Furthermore, the cable also has the ability to change the keyboard mapping, as well as

collect and build the identity of the USB device.



As mentioned, all of the above features are made possible thanks to a small chip placed inside the cable head. However, what makes OMG even more dangerous is that it looks very similar to a regular Lightning cable in both design and size. As you can see in the image above, the implanted chip takes up almost half of the space of the plastic shell, but still ensures the overall appearance of the cable and allows it to function properly. The video below shows how this malicious cable works.

Fortunately, the OMG cable is not intended to cause harm. It was developed by a security researcher nicknamed "MG", and serves as a penetration testing tool. This cable is now mass-produced and sold to cybersecurity supplier HaK5.