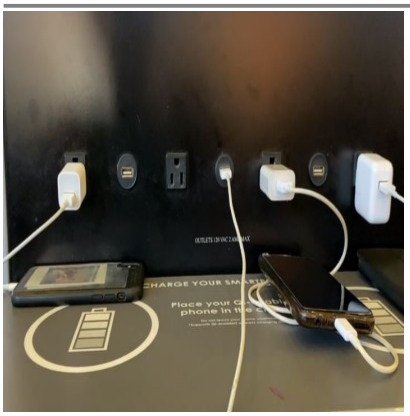
JOHN NOBLE
admin@johnnoble.co.uk



Juice Jacking – The dangers of using public USB charging stations

Description

JUICE JACKING

Travelers are advised to avoid using public USB power charging stations in airports, hotels, and other locations because they may contain dangerous malware, the Los Angeles District Attorney said in a security alert published last week.

USB connections were designed to work as both data and power transfer mediums, with no strict barrier between the two. As smartphones became more popular in the past decade, security researchers figured out they could abuse USB connections that a user might think was only transferring electrical power to hide and deliver secret data payloads.

This type of attack received its own name, as “juice jacking.”

Across the years, several proofs-of-concept were created. The most notorious is Mactans, presented at the Black Hat 2013 security conference, which was a malicious USB wall charger that could deploy malware on iOS devices.

Three years later, in 2016, security researcher Samy Kamkar took the concept further with KeySweeper, a stealthy Arduino-based device, camouflaged as a functioning USB wall charger that wirelessly and passively sniffs, decrypts, logs, and reports back (over GSM) all keystrokes from any Microsoft wireless keyboard in the vicinity.

Following Kamkar’s release of KeySweeper, the FBI sent out a nation-wide alert at the time, warning organizations against the use of USB chargers and asking companies to review if they had any such devices in use.

Also, in 2016, another team of researchers developed another proof-of-concept malicious USB wall charger. This one could record and mirror the screen of a device that was plugged in for a charge. The technique become known as “video jacking.”

Category

1. General
2. News
3. Security

Tags

1. security

Date Created
16/11/2024