Volume I Issue 13 Date: 16-03-2025

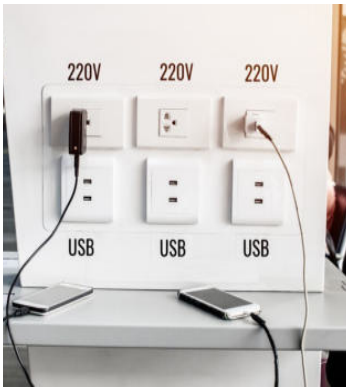
Cybersecurity Digest

Bi-weekly update by the CISO-Section of Meghalaya Rural Bank

Juice Jacking - The hidden danger

The term "juice jacking" was first coined in 2011 by investigative journalist Brian Krebs. It is a form of cyberattack where a public USB charging port is tampered with and infected using hardware and software changes to steal data or install malware on devices connected to it. The attack is used by hackers to steal users' passwords, credit card information, addresses, and other sensitive data stored on the targeted device.

Juice jacking attacks can take place in any public place with portable wall chargers, or public USB charging stations found in shopping malls, cafes, and hotels.



Juice jacking

How does juice jacking work?

To perform the attack, hackers infect USB ports or charging cables in public areas before the users connect to them. Most attacks target both Android and iOS mobile devices, with older devices being particularly vulnerable due to their outdated software. USB ports have multiple pins, but only one pin is used for charging while the other pins are used for data transfers. When users connect their devices to compromised USB ports, hackers use the connection to hack into mobile devices and steal personal data or deliver malware.

Types of Juice Jacking Attacks

Juice-jacking attacks can vary in their impact, even though the method remains the same. The different attack forms include data theft, malware installation, disabling attack, and multi-device attack.

In a data theft attack, hackers use juice-jacking to steal data from a device. The process is typically fully automated, and hackers often use crawlers to search the mobile device for personally identifiable information. Hackers may also use malicious apps to clone a device's data to another phone. However, cloning requires additional steps, such as a laptop as an intermediary to charge the targeted device.

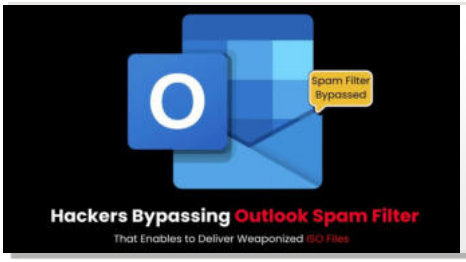
In a malware attack, hackers use charging ports to install malware or viruses on connected devices, which are then used to perform ransomware, spyware, or trojan attacks.

Inside this Digest

Juice Jacking– Prevention Tips

- **Avoid Public USB Ports:** Whenever possible, users should prioritize using a regular wall outlet with their own power adapter to charge their devices, eliminating the risk of data transfer or malware installation.
- **Carry a Power Bank:** Users can carry a portable power bank that they can keep charged beforehand, reducing their reliance on public charging stations.
- **Use a Charging-Only Cable:** Some companies sell special USB cables that only allow charging and block data transfer. While not foolproof, these cables can add a layer of protection.
- **Only Charge in Trusted Locations**: If users must use a public USB port, they should try to do so in a well-lit, populated area with security cameras.
- **Be Wary of Unfamiliar Ports**: Users should look for any signs of physical tampering with the charging port before plugging in their devices.
- **Monitor Your Device**: Users should stay vigilant while their device is charging and be mindful of any unusual activity or pop-up messages.

Cybersecurity News



A newly uncovered technique allows threat actors to bypass Microsoft Outlook's spam filtering mechanisms, enabling the delivery of malicious ISO files through seemingly benign email links.

This vulnerability exposes organizations to increased risks of phishing and malware attacks, particularly when combined with previously disclosed execution bypass methods.

Hackers can now access your bank account without OTP!!!

Cybercriminals have developed advanced methods to defraud individuals, bypassing the need for a One-Time Password (OTP) or ATM PIN. They are now leveraging deceptive messages containing fraudulent links that appear to be from legitimate banks. Once an unsuspecting recipient clicks on the link, their money is stolen without any OTP verification. The National Payments Corporation of India (NPCI) has issued a warning about a newly emerging scam involving call merging techniques, which fraudsters use to manipulate victims into unknowingly disclosing their OTPs, leading to financial fraud.

Scammers initiate a call, posing as a friend or acquaintance of the target. They claim to have obtained the victim's contact information through a mutual connection and request that they merge the call to include another individual. Unaware of the scam, the victim complies, inadvertently linking to a legitimate OTP verification call from their bank.

The fraudsters carefully time their calls so that when the victim receives an OTP, they assume it is related to the ongoing conversation and unwittingly share it. The criminals then use the OTP to authorize unauthorized transactions, resulting in financial losses for the victim.