Skillmine

infosec

Oct 2022

JUICE JACKING

Juice jacking is a cyber-attack in which a compromised Universal Serial Bus (USB) charging station transfers malware or steals personal information from a connected device. Juice jacking, also known as port jacking, affects any device that is charged via a USB plug.

Features of Juice Jacking Attacks:

01

Easy to implement this attack and can be undertaken by anyone.

02

There is no need to install additional software's on the phone because the attacker does not need any other software.

03

Less user conjecture: users are less aware of charging attacks than malware attacks.

04

Multi-platform: the attack is possible on iOS or Android phones.

How Juice Jacking Works?

- A hardware focused Man in the Middle attack is juice jacking.
- Malicious code or malware is installed on a smartphone and data can be copied from a smartphone via a specifically chosen charging station. This happens when one is using a data cable for both charging and data transfer. USB connectors have five pins, however only one is needed to charge to the connected device, and only two of the five are used for data transfer.
- The smartphone's charging port is secretly connected to the computer system and once a phone is put on charging, the hacker shall access the data present on the phone through the computer system.
- Photos, contacts, notes, browsing history, audio, video media and more become available to the infiltrator. In addition to copying or stealing data, hackers can also inject malware that can spy on and steal your data and secretly send it to the host computer.

Types of Juice Jacking Attacks

Data Theft:	In data theft attacks, users are left unaware that their sensitive information has been stolen. Depending on how long the device is plugged into the compromised cable or port, vast amounts of data can be compromised. With enough time and storage space, hackers can back up all the data on the device.
Malware Installation:	When malware installation juice-jacking attacks occur, the malware placed on the device can cause a lot of damage, including phone or computer spoofing, tracking the user, locking the user out of the device, or stealing information.
Multi device Attack:	In addition to harming a device plugged into a compromised charger, a device charged with a tainted cable can infect other cables and ports with the same malware as an unknown carrier of the virus.
Disabling Attack:	Some malware uploaded through a charging device can block owners from accessing their devices, giving hackers full access.

How to Determine the Victim of Juice Jacking?

Victims are often unaware that they have been "juice jacked", but there are some tell-tale signs that a device may be compromised. The device may:

- Consume more battery life than usual
- Operate at a slower speed
- Take longer to load
- Frequent crashes due to abnormal data usage

Counter Measures:

1. Never use a free USB port or charging cable. Carry your charging adapter and cable during travel.
2. Investing in a power bank is advisable, as it is one of the most convenient and safest bets.
3. If you insist on charging your device via a USB port, it is recommended you should purchase "USB condoms". They provide an additional layer of security and protection between the port and the mobile device.
4. Turn off the phone before connecting it to a public phone charging station.
5. Use a charge-only USB adaptor that allows devices to be charged but does not transfer data.
6. Decline data transfer requests.
7. Use two-factor authentication or biometric logins when available.
8. Keep the software updated. Software updates will likely feature up-to-date security protection, patches, and bug fixes. For example: Many updated mobile phones require permission before allowing data transmission when plugged into an unknown station or device.

Some examples introduced within the last decade:

2011
An experiment conducted by Aires Security at DefCon was the first occurrence.

2012
A form of attack utilizing USB OTG (on-the-go) identified features, one that would unlock the charged phone and steal the authentication keys to their Google account.

2013
This year's Black Hat conference saw the debut of a novel USB hacking idea that implanted a Trojan inside phones.

2015
A power adapter will decode and record all keystrokes from any displayed Microsoft wireless keyboard.

Epilogue

- This practice is a threat to individual consumers and businesses as society becomes increasingly dependent on mobile devices. While not as prominent or widespread as a threat like phishing and ransomware attacks, it is still something to be aware of.
- Anti-virus software can provide additional protection, but it won't help in the event of a juice hack. However, anti-virus software can block the apps if a cybercriminal tries to install malware.
- Be cautious where electronic devices are charged. Public charging stations at airports, hotels and restaurants are a prime target for cybercriminals to juice jack and collect sensitive information or install malware to further criminal activity.

Beware of charging your phone at charging stations. Hackers could be waiting!
Be Vigilant. Be Safe. #JUICEJACKING #USBJACKING

SKILLMINE CYBER SECURITY TEAM

Skillmine
Technology • Consulting • Services

#46/4, Novel Tech park, Kudlu Gate, Bangalore Karnataka 560 068

+91 9920663515
www.Skill-mine.com
info@Skill-mine.com

India | KSA | UK | USA