FBI Warns of Public Charging Station Vulnerabilities

The FBI recently released a warning to avoid free public charging stations as they are potentially being compromised by threat actors. Cyber criminals are using public charging stations to infect devices with malware or monitoring software that enables the threat actor to access your phone, tablet, or computer, also referred to as "Juice Jacking." These charging stations are popular in airports, malls, and hotels and provide threat actors with unsuspecting victims. The malicious malware or monitoring software is downloaded through the USB charging ports and allows threat actors to primarily collect usernames and passwords, and to lock a device if they deem it is beneficial. Information gained is then used by the threat actor to drain accounts or sell to other cyber criminals for future exploitation.

Juice jacking provides the victim with no indication that their device has been compromised. The best way for individuals to avoid this threat is to bring their own charging device/battery pack or their own USB cable that plugs into an outlet for public charging. Additionally, never use a charging cord that has been left behind and avoid using USB charging stations when possible. Organizations should be aware of new tactics used by threat actors and provide education and training to their employees on how to mitigate vulnerabilities.

The Critical Start Cyber Threat Intelligence (CTI) team will continue to monitor the situation and work closely with the Threat Detection Engineering (TDE) team and the SOC to implement any relevant detections. For future updates, the CTI team will post via ZTAP® Bulletins and on the Critical Start Intelligence Hub.

References:

1. https://www.cbsnews.com/news/fbi-warns-against-juice-jacking-what-is-it/
2. https://www.cnbc.com/2023/04/10/fbi-says-you-shouldnt-use-public-phone-charging-stations.html