PHY-2 · Mobile Threat Catalogue

Archived: 2026-04-06 00:23:40 UTC

Mobile Threat Catalogue

Device Attack via PC Connection

Contribute

Threat Category: Physical Access

ID: PHY-2

Threat Description: Compromised PCs may try to exploit a trusted USB connection between a mobile device and the PC, and infect the mobile device.

Threat Origin

Exploiting Smart-Phone USB Connectivity for Fun and Profit [1]

Exploit Examples

New Malware Tries to Infect Android Devices Via USB Cable [2]

CVE Examples

Not Applicable

Possible Countermeasures

Mobile Device User

When charging a device, avoid connecting mobile devices directly to computers, and prefer the use of simple corded chargers obtained directly from the device vendor.

To prevent some attacks over USB connectivity, disable USB debugging on Android devices when that feature is not in use.

To reduce the opportunity for an attacker to directly connect a device to a malicious computer, use strong physical security when a device is being left directly unattended (e.g., lock it in a secure container).

To prevent some attacks over USB connectivity, ensure the device has an unlock code set and is explicitly locked when being left directly unattended.

References

1. Z. Wang and A. Stavrou, “Exploiting Smart-Phone USB Connectivity for Fun and Profit”, in Proceedings of 26th Annual Computer Security Applications Conference, 2010, pp. 357-365; https://dl.acm.org/doi/pdf/10.1145/1920261.1920314?casa_token=5XmsJ5lz06EAAAAA:HavUpmf81lNQ74ooinjWS1BZkQMkfhsbWJwFwa3UEieHGYKTCmv-TSwwaHRQhz-I4XFzdzkDHEOA [accessed 8/1/2022] ↩

2. G. Sims, “New Malware Tries to Infect Android Devices Via USB Cable”, 27 Jan. 2014; www.androidauthority.com/new-malware-tries-infect-android-devices-via-usb-cable-339356/ [accessed 8/31/2016] ↩
