LPN-0 · Mobile Threat Catalogue

Archived: 2026-04-05 19:55:18 UTC

Mobile Threat Catalogue

Rogue Access Points

Contribute

Threat Category: Network Threats: Wi-Fi

ID: LPN-0

Threat Description: Public, unsecure access points are subject to rogue access point attacks. This could allow adversaries to man-in-the-middle traffic going to and from devices connected to the network.

Threat Origin

Guidelines for Securing Wireless Local Area Networks (WLANs) (SP 800-153) [1]

Exploit Examples

Darkhotel: A Sophisticated New Hacking Attack Targets High-Profile Hotel Guests [2]

CVE Examples

Possible Countermeasures

Mobile Device User

Avoid the use of untrusted and unencrypted Wi-Fi networks, particularly when needing to access sensitive services.

When needing to connect to untrusted and unencrypted Wi-Fi networks, attempt to verify with a representative of the hosting organization (e.g., coffe shop employee) that the detected network is the correct one.

To reduce the probability of connecting to rogue access points, use Wi-Fi hotspot services that associate access points with registered Wi-Fi provider, geolocation, and crowd-sourced reputation data to make assertions about the their apparent trustworthiness.

Enterprise

To reduce the probability of connecting to rogue access points, use Wi-Fi hotspot services that associate access points with registered Wi-Fi provider, geolocation, and crowd-sourced reputation data to make assertions about the their apparent trustworthiness.

To avoid this threat, only allow mobile devices to connect to authorized Wi-Fi networks that use WPA2 encryption.

References
