Cellular, Bluetooth, WiFi, IoT Spyware

Invisible Threats, Visible Protection

LOCH TECHNOLOGIES

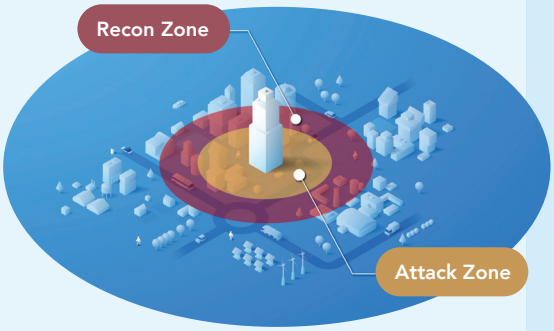
Gartner COOL VENDOR 2021

With 80% of new IoT deployments wireless, wireless is the new network and new attack surface.

Enforce Zero Trust to detect, assess and prevent risk.

CELLULAR ATTACKS

- **Malicious SMS** - attacks on mobile-based messaging applications to engage in cyberattacks. Covert data exfiltration is the goal.
- **Malware / BOTNETs** - stealthy attacks on devices that change behaviour state and data utilization. Excessive data plan usage.
- **Fake Cell Towers Detection** - protection against rogue base stations and IMSI catchers that lure authorized cellular clients to a fake 4G/5G network for further manipulation.
- **Misconfigurations** - UE (user equipment) and IoT devices can lead to rogue communications and data exfiltration. Holistic protection for both mobile and IoT.
- **SIM Port Swap/Hi-Jacking** - classify all assets using SIM connections to prevent fraud and excessive data plan over billing.



Wi-Fi ATTACKS

- **Rogue Access Points** - are connected to an authorized network, usually with an open SSID, allowing attackers to bypass perimeter security for covert data exfiltration.
- **Rogue clients** - are defined as clients that connect to a rogue or other malicious access point within range of a private network.
- **Neighbor access point** - are independent networks that are not under administrative control and could be used to bypass internal security controls.
- **Ad-hoc Connections** - are peer to peer and mesh WiFi, such as Apple AirDrop, between clients that can circumvent security controls and allow clients to evade firewalls and policies.
- **Evil twins** - are access points mimicking a legitimate AP by spoofing its network to perform data collection, malware delivery and man-in-the-middle attacks.
- **Misconfigured Access Points** - connected to your private network with a configuration that does not conform to security policies.

IoT ATTACKS

- **Off Network devices** - are devices such as spy cameras and drones which do not connect to an approved network but can lead to data exfiltration.
- **Shadow IoT** - are autonomous networks on non-standard frequencies like 900Mhz i.e HVACs, and Smart Buildings. Existing security tools lack visibility to discover and audit this risk profile.
- **Nefarious near-field and far-field covert wireless communications (bugs)** - are running on non standard frequencies can lead to data exfiltration.
- **CBRS and Private LTE deployments** - are non-carrier cellular networks vulnerable to UE and protocol attacks.
- **Home / Consumer IoT** connected to enterprise networks creating back-door loopholes.

info@loch.io | 1-888-725-9434 | www.loch.io