SilentAir Group Abuses Asian Telecom Networks to Intercept SMS Codes



Enea reports a state-level spying group, SilentAir, used compromised equipment inside Asian mobile operators to intercept calls and texts of selected targets, mostly in Taiwan.

- Enea, a Stockholm-based telecom and cybersecurity software company, named the group SilentAir.
- The group used hacked equipment inside Asian mobile operators to intercept calls and texts.
- Targets were selected individuals, mostly in Taiwan.
- Attack sources were traced to at least six Asian countries.
- Enea assessed with high confidence that SilentAir is a state-level actor.

What was reported

Enea, a telecom and cybersecurity software company based in Stockholm, has identified a new spying group it calls SilentAir. According to the report, the group used compromised equipment inside mobile operators in Asia to intercept the calls and text messages of selected people, mostly in Taiwan.

Enea found the group's attack sources in at least six Asian countries and assessed with high confidence that SilentAir is a state-level actor.

Why it matters for 2FA

The headline of the report points to interception of SMS-based two-factor authentication codes. When messages are read inside the carrier network, the code reaches the attacker as well as the user, regardless of how well the handset or the user's own device is protected. The source excerpt does not give further technical detail, so the exact methods and the full list of affected operators remain unclear.

Practical reading for Saudi institutions

The reported targeting was selective and focused on Taiwan, and the source does not mention Saudi Arabia. Even so, the case is a useful reminder that SMS is a weaker second factor for high-value accounts, particularly for executives, administrators and staff who travel or roam on foreign networks. Institutions should review where SMS codes still protect sensitive access and plan a move to stronger methods.

What to do now

1. Inventory systems and accounts where SMS codes are still the second factor, starting with privileged and executive accounts.
2. Move high-risk users to app-based authenticators, hardware security keys or other phishing-resistant methods.
3. Review remote and roaming access for staff who travel, and apply stricter controls for sign-ins from foreign networks.
4. Ask your mobile operators how they protect signaling and core network equipment and how they notify customers of suspected interception.
5. Include SMS interception in your threat model and update authentication standards under your NCA ECC and SAMA CSF programs.