Suspected Vietnam-linked group targets Southeast Asian bodies in South China Sea espionage



SOCRadar has detailed a previously undocumented campaign, WeaveLotus, attributed to a Vietnam-sponsored group targeting Southeast Asian military, government and legislative bodies to gather intelligence on South China Sea defense matters.

- SOCRadar codenamed the previously undocumented activity set WeaveLotus.
- The group is described as Vietnam-sponsored; the report frames the attribution as suspected.
- Targets are military, government and legislative organizations in Southeast Asia.
- The stated aim is intelligence on South China Sea defense and military agreements.
- The activity is assessed to include five intrusions in Thailand.

SOCRadar has described a previously undocumented set of intrusions that it has codenamed WeaveLotus. The activity is attributed to a hacking group assessed to be sponsored by Vietnam, and the objective is espionage rather than financial gain.

What was reported

According to the report, the group went after military, government and legislative organizations in Southeast Asia. The intent was to collect intelligence on defense and military agreements connected to the South China Sea. The activity is assessed to include five intrusions in Thailand.

The source excerpt does not provide technical details such as the intrusion methods, tools or indicators, and it does not name the affected organizations. We therefore make no claims on those points.

Relevance for Saudi institutions

There is no indication in the source that organizations in the Kingdom were targeted. The case is still a useful reminder that state-linked espionage tends to focus on bodies that hold sensitive policy, defense and diplomatic information. Government entities, defense suppliers and institutions that exchange information with them should consider whether they hold comparable material.

A sensible response is to review existing controls rather than react to this single report. Once SOCRadar's full technical findings are available, security teams can compare them against their own monitoring.

What to do now

1. Obtain SOCRadar's full WeaveLotus report and check any published indicators against your logs and detection tools.
2. Identify which systems and mailboxes hold defense, policy or diplomatic information and confirm they are monitored and access-restricted.
3. Review the security of exchanges with partners and suppliers who handle sensitive government or defense material.
4. Brief executive and legal-affairs staff on targeted phishing aimed at people with access to policy information.
5. Confirm your threat-intelligence process covers state-linked espionage activity and feeds incident response.