TELEMAR

# APT:
# The silent attack with long-term consequences

An Advanced Persistent Threat (APT) refers to prolonged, sophisticated cyberattacks typically carried out by well-organised, highly skilled groups - often backed by nation states or large sponsors. The goal isn't a quick breach, but silent infiltration, long-term presence, and the pursuit of broader objectives such as data theft, espionage, sabotage, or disruption of critical infrastructure.

## Why it's particularly dangerous in maritime and energy sectors

APT attacks are stealthy and multi-phased. The attacker first gathers intelligence, on network architecture, software, devices, and personnel, then crafts a targeted operation that may remain dormant for weeks or months before activation. In systems with limited oversight or internet access, such as vessels or offshore platforms, these attacks can go unnoticed until it's too late.

## Examples from the field

- An attacker passively monitors fleet movement patterns for months to support geopolitical intelligence gathering
- A trojan is embedded in a shoreside IT system and activates upon vessel docking, enabling data exfiltration
- ICS (Industrial Control Systems) software on a platform is covertly altered to allow remote sabotage at a critical moment

## How to defend against it

- Enable 24/7 monitoring with our security operations centres and advanced threat analytics
- Implement a layered defense approach: system isolation, detailed logging, and strict access controls
- Conduct regular forensic analysis and threat hunting, especially for high risk or mission-critical systems; enable deep packet inspection on UTM services that have the capability to detect Advanced Persistent Threats.

APT attacks aren't loud, they are patient, calculated, and highly targeted. That's why they require a proactive defence strategy and continuous vigilance.

**Contact us**
Email: Sos@telemargroup.com
www.telemargroup.com