Geopolitical tensions Key Indicator of Compromise

Tracking ID#: PCS-03-1426

Date: 14-03-2026

Disclaimer: This is a shared security advisory service; hence, it can be communicated to a single dedicated point of contact. We would highly appreciate it if you assigned them to your organisation's concerned asset/technology owner. Please use it as applicable to your environment

Date: 14-03-2026

Summary:

Recent threat intelligence indicates the emergence of a destructive cyber campaign identified as **Snowdrop Wiper**, which has been observed targeting organizations within the **United Arab Emirates (UAE)**. The activity has been associated with threat actors believed to be linked to Iranian operations and is considered a high-severity threat due to its destructive capabilities. The campaign utilizes a wiper-type malware designed to disrupt systems by permanently deleting or corrupting critical data, potentially rendering affected systems inoperable and causing significant operational disruption.

The indicators associated with this campaign suggest a focused targeting of regional entities, with the objective of causing large-scale service disruption and damaging critical infrastructure. Due to the destructive nature of wiper malware, successful compromise could lead to data loss, system downtime, and operational impact across affected environments. The activity is assessed as part of a broader cyber operation linked to ongoing geopolitical tensions in the region.

Target:

Applicable to all users.

Mitigation Recommendations:

Recommended to block all the IOCs mentioned in the attached excel sheet.