Severity

High

Analysis Summary

OilRig, aka HelixKitten, APT 34, and Twisted Kitten, is a suspected Iranian threat group targeting Middle Eastern and international victims since at least 2014. The group appears to conduct supply chain attacks, taking advantage of the trust connection between organizations to attack its major targets. Based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that corresponds with nation-state goals, researchers conclude that the organization operates on behalf of the Iranian government. Financial, political, energy, chemical, and telecommunications sectors are the top targets of this threat actor group. For lateral movement, OilRig makes use of stolen account credentials. OilRig uses credential dumping tools like Mimikatz to harvest credentials from accounts logged onto the compromised system after gaining access to it. The threat actor group utilizes these credentials to gain access to and move laterally via the network's systems.

Impact

Information Theft and Espionage Exposure of Sensitive Data

Indicators of Compromise

MD5

- ccc36ffd7b4634b107e3f8518ad3a539

SHA-256

- b69812221cd9328a70c90f771c58be44693de493df18f0a08ebd0bb6236e37a7

SHA-1

- c7a1f076dfaeaaa6bacc0e610078a20f1879f091

Remediation

Block all threat indicators at your respective controls. Search for IOCs in your environment.