MITRE-ID: G0049

Name: OilRig

Country: Iran

Description: OilRig is a suspected Iranian threat group that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of sectors, including financial, government, energy, chemical, and telecommunications. It appears the group carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets. The group works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests.

TTPs:

Initial Access:

* spearphising emails with malicious attachments was sent to potential victims using compromised and/or spoofed email accounts
* use compromised credentials to access other systems on a victim network

Execution:

* use PowerShell scripts for execution, including use of a macro to run a PowerShell command to decode file contents
* created scheduled tasks that run a VBScript to execute a payload on victim machines.

Persistence:

* use remote services such as VPN, Citrix, or OWA to persist in an environment.
* abuse the Outlook Home Page feature for persistence

Defense Evasion:

* run a PowerShell command to decode file contents
* delete files associated with their payload after execution

Credential Access:

* use tools to dump passwords from web browsers
* use keylogging tools

Discovery:

* use net.exe in a script to find the password policy of a domain.
* use macros to verify if a mouse is connected to a compromised machine

Lateral Movement:

* use Remote Desktop Protocol for lateral movement
* use Putty to access compromised systems

Collection:

* use a tool to capture a screenshot of user's desktop

Command and control:

* use DNS for C2 including the publicly available tunneling service