The APT33 group, suspected to be from Iran, has launched a new campaign targeting the energy sector organizations.

The attack utilizes Shamoon malware, known for its destructive capabilities. The threat actor exploited a vulnerability in the network perimeter to gain initial access.

The malware was delivered via spear-phishing emails containing a malicious attachment. The malware’s behavior was observed communicating with IP address 192.168.1.1 and domain example.com. The attack also involved lateral movement using PowerShell scripts.