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.

The "EOF marker not found" error typically occurs when the PDF file is incomplete or corrupted. This issue can arise due to problems in the PDF structure, missing end markers, or using a non-standard or partially downloaded PDF file.

Here's how to resolve or work around this issue:

In today's world of cybersecurity, organizations rely heavily on threat reports to identify potential risks, understand malicious activities, and make informed decisions to defend their networks. These reports, often written in natural language, contain valuable intelligence such as Indicators of Compromise (IoCs), Tactics, Techniques, and Procedures (TTPs), and other critical data points. However, manually extracting this information can be a daunting task due to the unstructured nature of these reports. This is where Natural Language Processing (NLP) comes into play, enabling the automation of threat intelligence extraction and analysis.
To get started, we will focus on one of the most prominent cybersecurity frameworks used to identify and categorize malicious behavior: the MITRE ATT&CK Framework. This framework categorizes adversarial actions into various tactics and techniques that reflect common behaviors of advanced threats.
In this challenge, you will develop a function that extracts key threat intelligence from a natural language threat report.

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.