Threat Name: PDF_File_Detection

Threat Category: File Type Identification

Threat Description: The YARA rule PDF_File detects PDF documents based on their file signature (magic number).

Indicators of Compromise (IoCs):

File header: { 25 50 44 46 } (PDF signature)

Detection Mechanism: Matches PDF files by checking their header bytes.

Possible Attribution & Use Cases: Used in malware embedded in PDF files (e.g., malicious attachments).

Recommended Actions: Scan detected PDFs for embedded scripts or exploits.