

Threat Name: Text_File_Detection

Threat Category: Generic File Classification

Threat Description: The YARA rule Text_File_Detection is used to detect the presence of text files based on their extensions, specifically ".txt".

Indicators of Compromise (IoCs):

.txt string within a filename or file metadata.

Detection Mechanism:

Matches file names containing ".txt", useful for text file identification.

Possible Attribution & Use Cases:

Used in categorizing file types rather than detecting malware.

Recommended Actions:

Combine with content-based detection rules for enhanced threat analysis.