Threat Name: Email_Address_Detection

Threat Category: Phishing & Spam Analysis

Threat Description: The YARA rule Email_Address_Detection detects email addresses in files based on a regular expression pattern that matches ?.com?, ?.net?, and ?.org? domains.

Indicators of Compromise (IoCs):

Regex pattern for email addresses in common domains.

Detection Mechanism:

Matches email addresses within documents, logs, and scripts.

Possible Attribution & Use Cases:

Used to detect phishing emails or malware command & control communications.