Threat Name: IP_Address_Detection

Threat Category: Network Indicator Matching

Threat Description: The YARA rule IP_Address_Detection detects IPv4 addresses present within files. It uses a regular expression to match standard IP address formats.

Indicators of Compromise (IoCs):

Regex pattern for IPv4 addresses.

Detection Mechanism:

Identifies hardcoded IPs in scripts, logs, or binaries.

strings: $ip = /\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}/

Possible Attribution & Use Cases:

Used to track malware C2 infrastructure.

Recommended Actions:

Cross-check detected IPs against threat intelligence feeds.