Threat Name: Basic_String_Match

Threat Category: Basic Malware Detection

Threat Description:

The YARA rule Basic_String_Match is a simple string-matching rule designed to detect the presence of malware-related keywords within files. It searches for the words "malware" and "infected", which are commonly used in malicious binaries, scripts, or logs.

Indicators of Compromise (IoCs):

Hardcoded strings:

"malware"

"infected"

Detection Mechanism:

Identifies files containing these keywords, regardless of encoding or formatting.

Possible Attribution & Use Cases:

Used as a basic heuristic rule for initial malware triage.