Threat Name: Basic_JS_Detection

Threat Category: Suspicious JavaScript Activity

Threat Description: The YARA rule Basic_JS_Detection detects JavaScript code snippets that are commonly found in web-based malware and browser exploits.

Indicators of Compromise (IoCs):

"function"

"var "

"document.write"

Detection Mechanism:

Flags JavaScript files with at least two of these keywords.

Possible Attribution & Use Cases:

Used in malicious JavaScript payloads for drive-by attacks.

Recommended Actions:

Perform static code analysis to detect obfuscated JavaScript payloads.