Threat Name: Base64_Content_Detection

Threat Category:

Data Obfuscation

Steganography

Threat Description:

The YARA rule Base64_Content detects long Base64-encoded strings, which may be used for data obfuscation, malware payload encoding, or exfiltration techniques.

Indicators of Compromise (IoCs):

Regex pattern for Base64-encoded data: [A-Za-z0-9+/]{30,}

Detection Mechanism:

Matches Base64-encoded text patterns in files, scripts, and logs.

Possible Attribution & Use Cases:

Used in malware payload encoding to evade detection.

Recommended Actions:

Inspect Base64 content for encoded payloads or scripts.