Threat Name: Password_String_Detection

Threat Category:

Potential Credential Exposure

Threat Description: The YARA rule Password_String_Detection looks for plain-text credentials in files by detecting the words "password" or "passwd".

Indicators of Compromise (IoCs):

"password"

"passwd"

Detection Mechanism:

Matches files containing plain-text password references.

Possible Attribution & Use Cases:

Used in identifying leaked credentials in logs or scripts.

Recommended Actions:

Encrypt or hash passwords instead of storing them in plaintext.