Threat Name: Simple_Backdoor_Detection

Threat Category: Remote Access Malware

Threat Description:

The YARA rule Simple_Backdoor detects text-based indicators of backdoor functionality, which may indicate remote access tools (RATs).

Indicators of Compromise (IoCs):

"shell", "backdoor", "remote access"

Detection Mechanism:

Matches keywords related to backdoor functionalities.

Possible Attribution & Use Cases:

Used in covert remote access malware.

Recommended Actions:

Investigate suspicious remote access activity.