Threat Name: Basic_Command_Detection

Threat Category: Suspicious Process Execution

Threat Description: The YARA rule Basic_Command_Detection is designed to detect command-line execution of "cmd.exe" and "powershell.exe", which are often abused in malware execution and Living Off The Land Binaries (LOLBins).

Indicators of Compromise (IoCs):

"cmd.exe"

"powershell.exe"

Detection Mechanism:

Matches command execution strings in logs, memory, or script files.

Possible Attribution & Use Cases:

Used in command injection attacks and script-based malware.