Threat Name: Batch_File_Detection

Threat Category: Script File Classification

Threat Description: The YARA rule Batch_File detects Windows batch scripts based on common batch file keywords.

Indicators of Compromise (IoCs):

.bat (Batch file extension)

"echo"

"rem " (Batch file comments)

Detection Mechanism:

Identifies batch scripts used in automation or malware execution.

Possible Attribution & Use Cases:

Used in Windows malware droppers and batch-based exploits.

Recommended Actions:

Monitor batch file executions for signs of automation abuse.