Threat Name: Script_Detection

Threat Category: Scripting Engine Identification

Threat Description: The YARA rule Script_Detection identifies script files that use common shebang lines (#!), indicating execution via Bash, Python, or Perl.

Indicators of Compromise (IoCs):

#!/bin/bash

#!/usr/bin/python

#!/usr/bin/perl

Detection Mechanism: Matches scripts using standard shebang lines.

Possible Attribution & Use Cases: Used in identifying suspicious script executions.

Recommended Actions: Monitor for unauthorized script execution in sensitive environments.