Threat Category: Malware Backdoor

Threat Description: The rule is designed to detect connections originating from systems infected with the HackAttack 1.20 backdoor. This rule focuses on traffic from an internal network to an external network on TCP port 31785. The detection mechanism involves checking for the presence of the string "host" within the TCP packet payload. This string is a characteristic marker used by the HackAttack 1.20 backdoor during communication.

Indicators of Compromise (IoCs):

TCP Port: 31785

Content Pattern: "host"

Detection Mechanism:

This rule identifies potential HackAttack 1.20 backdoor activity using the following conditions:

The network protocol must be TCP.

The traffic direction must be from $HOME_NET to $EXTERNAL_NET.

The source port must be 31785.

The TCP connection must be established (established).

The payload must contain the string "host".

Possible Attribution & Use Cases:

The detection can be used to identify systems infected with the HackAttack 1.20 backdoor.

This rule is useful for monitoring network traffic for malicious activity related to backdoor software.

Recommended Actions:

Monitor and Investigate: If this rule is triggered, investigate the affected systems to confirm the presence of the HackAttack 1.20 backdoor.

Containment: Isolate any infected systems to prevent further unauthorized access or activity.

Remediation: Remove the HackAttack 1.20 backdoor from infected systems.

Network Security: Implement intrusion detection and prevention systems to block known backdoor traffic.

Author & Attribution:

Rule Author: Community

Rule Source: Community

Rule SID: 141

Rule Revision: 10