Threat Category: Malware, Backdoor, Trojan

Threat Description: The rule is designed to detect connections originating from systems infected with the NetSphere backdoor. This rule focuses on traffic from an internal network to an external network on TCP ports between 30100 and 30102. The detection mechanism involves checking for the presence of the string "NetSphere" within the TCP packet payload. This string is a characteristic marker used by the NetSphere backdoor during communication.

Indicators of Compromise (IoCs):

TCP Ports: 30100-30102

Content Pattern: "NetSphere"

Detection Mechanism: This rule identifies potential NetSphere 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 within the range of 30100 to 30102.

The TCP connection must be established (established).

The payload must contain the string "NetSphere".

Possible Attribution & Use Cases: This rule is useful for monitoring network traffic for malicious activity related to backdoor software.

Recommended Actions:

Remediation: Remove the NetSphere backdoor from infected systems.

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

Vulnerability Management: Ensure that systems are patched and up-to-date to prevent exploitation of vulnerabilities that could lead to backdoor infections.

Author & Attribution:

Rule Author: Community

Rule Source: Community

Rule SID: 146

Rule Revision: 13