Threat Category: Protocol Anomaly, RPC Portmap Decode

Threat Description: The rule is designed to detect attempts to make an AMD (Automount) TCP pid request using RPC. This rule focuses on traffic from an external network to an internal network on TCP port 500 (and potentially others). The detection mechanism involves checking for specific byte sequences within the TCP packet payload at specific offsets and depths. Specifically, it checks for "|00 04 93 F3|" at a depth of 4 and offset of 16, "|00 00 00 09|" within 4 bytes with a distance of 4, and "|00 00 00 00|" at a depth of 4 and offset of 8. These patterns are indicative of a request to the automount service.

Indicators of Compromise (IoCs):

TCP Port: 500

Content Pattern 1: "|00 04 93 F3|" (depth 4, offset 16)

Content Pattern 2: "|00 00 00 09|" (within 4, distance 4)

Content Pattern 3: "|00 00 00 00|" (depth 4, offset 8)

Detection Mechanism:

The network protocol must be TCP.

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

The destination port must be 500.

The TCP connection must be established.

Possible Attribution & Use Cases:

The detection can be used to identify reconnaissance or exploitation attempts targeting the automount service.

This rule is useful for monitoring network traffic for potentially malicious RPC activity.

Recommended Actions:

Monitor and Investigate: If this rule is triggered, investigate the source of the traffic and the targeted system to determine the intent of the automount request.

Restrict Access: Implement firewall rules to restrict access to automount services from untrusted networks.

Disable Automount: If possible, disable the automount service if it is not required.

Author & Attribution:

Rule Author: Community

Rule Source: Community

Rule SID: 1953

Rule Revision: 10