Threat Category: Malware, Backdoor

Threat Description: The SNORT rule is designed to detect access attempts to the Doly 2.0 backdoor. This rule focuses on traffic from an internal network to an external network on TCP port 6789. The detection mechanism involves checking for the presence of the string "Wtzup Use" within the TCP packet payload at a depth of 32 bytes. This string is a characteristic marker used by the Doly 2.0 backdoor.

Indicators of Compromise (IoCs):

TCP Port: 6789

Content Pattern: "Wtzup Use" (depth 32)

Detection Mechanism:

This rule identifies potential Doly 2.0 backdoor activity using the following conditions:

The network protocol must be TCP.

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

The TCP connection must be established (established).

The payload must contain the string "Wtzup Use" at a depth of 32 bytes.

Recommended Actions:

Monitor and Investigate: If this rule is triggered, investigate the affected systems to confirm the presence of the Doly 2.0 backdoor.

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

Remediation: Remove the Doly 2.0 backdoor from infected systems.

Rule Author: Community

Rule Source: Community

Rule SID: 119

Rule Revision: 11