Threat Category: Malware, Backdoor, Attempted Administrator Access

Threat Description: The rule is designed to detect attempts to exploit systems using the "w00w00" backdoor. This detection focuses on identifying TCP traffic containing the specific string "w00w00," which is associated with attempts to gain unauthorized access via the w00w00 backdoor, often targeting Telnet services.

Indicators of Compromise (IoCs)

Content: "w00w00"

Detection Mechanism:

The traffic is TCP.

The traffic flow is from the server to the client and the TCP connection must be established (to_server,established).

The destination port is 23 (Telnet).

The rule checks for the presence of the string "w00w00" in the packet's content.

Possible Attribution & Use Cases:

The detection indicates a possible attempt to exploit the w00w00 backdoor.

w00w00 is a type of backdoor that allows unauthorized access and control of the compromised system, frequently used to target Telnet servers.

This rule can be used to identify and block attempts to exploit the w00w00 backdoor.

Recommended Actions:

Monitor and Investigate: Analyze the traffic and the involved systems to confirm the attempted exploitation of the w00w00 backdoor.

Containment & Mitigation: Isolate the affected system to prevent further spread. Secure the Telnet

service or discontinue its use if possible.

Author & Attribution:

Rule Author: community

Ruleset: community

SID: 209

Revision: 9