Threat Category: Malware, Backdoor, Attempted Administrator Access

Threat Description: The rule is designed to detect generic attempts to access systems using a backdoor. This detection focuses on identifying TCP traffic containing the string "backdoor," which is a common string used in various backdoor access attempts, often targeting Telnet services. The rule ignores case sensitivity.

Indicators of Compromise (IoCs)

Content: "backdoor" (case-insensitive)

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 "backdoor" (case-insensitive) in the packet's content.

Possible Attribution & Use Cases:

The detection indicates a possible generic attempt to access a system via a backdoor.

Backdoors allow unauthorized access and control of compromised systems.

This rule can be used to identify and block generic backdoor access attempts, particularly those targeting Telnet.

Recommended Actions:

Monitor and Investigate: Analyze the traffic and the involved systems to confirm the attempted backdoor access.

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: 210

Revision: 7