Threat Category: Malware / Backdoor

Threat Description: This rule is designed to detect network traffic associated with the Dagger 1.4.0 backdoor. This rule identifies specific communication patterns indicative of this malware's activity. The detection focuses on traffic from the internal network to an external network over TCP port 2589. The rule checks for a specific content pattern within the payload of the TCP packet, specifically the presence of the string "2|00 00 00 06 00 00 00|Drives|24 00|" at a depth of 16 bytes. This pattern is characteristic of the Dagger 1.4.0 backdoor's communication protocol.

Indicators of Compromise (IoCs):

TCP Port: 2589

Content Pattern: "2|00 00 06 00 00 00|Drives|24 00|" (at depth 16)

Detection Mechanism: This rule identifies potential Dagger 1.4.0 backdoor activity using the following conditions:

The network protocol must be TCP.

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

The destination port must be 2589.

The TCP connection must be established (established).

The payload must contain the specific content pattern "2|00 00 00 06 00 00 00|Drives|24 00|" at a depth of 16 bytes.

Possible Attribution & Use Cases: The detection can be used to identify systems infected with the Dagger 1.4.0 backdoor. This rule is useful for monitoring network traffic for malicious activity related to known backdoor software.

Recommended Actions:

Monitor and Investigate: If this rule is triggered, investigate the affected systems to confirm the presence of the Dagger 1.4.0 backdoor.

Containment: Isolate any infected systems to prevent further spread of the malware.

Remediation: Remove the Dagger 1.4.0 backdoor from infected systems and restore affected files.

Author & Attribution:

Rule Author: Community

Rule Source: Community

Rule SID: 105

Rule Revision: 14