Threat Category: Malware Backdoor

Threat Description: The rule is designed to detect connection requests related to the Infector 1.6 backdoor. This rule focuses on traffic from an external network to an internal network on TCP ports between 1000 and 1300. The detection mechanism involves checking for the presence of the string "FC " within the TCP packet payload. This string is a characteristic marker used by the Infector 1.6 backdoor during initial connection requests.

Indicators of Compromise (IoCs):

TCP Ports: 1000-1300

Content Pattern: "FC "

Detection Mechanism:

This rule identifies potential Infector 1.6 backdoor connection requests using the following conditions:

The network protocol must be TCP.

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

The destination port must be within the range of 1000 to 1300.

The TCP connection must be established (established).

The payload must contain the string "FC ".

Possible Attribution & Use Cases:

Recommended Actions:

Remediation: Remove the Infector 1.6 backdoor from infected systems.

Network Security: Implement intrusion detection and prevention systems to block known backdoor traffic.

Vulnerability Management: Ensure that systems are patched and up-to-date to prevent exploitation

of vulnerabilities that could lead to backdoor infections.

Author & Attribution:

Rule Author: Community

Rule Source: Community

Reference: Nessus-11157

Rule SID: 121

Rule Revision: 14