Threat Category: Malware, Backdoor

Threat Description: The SNORT rule is designed to detect connections originating from systems infected with the Back Construction 2.1 backdoor. This rule focuses on traffic from an internal network to an external network on TCP ports 5401 and 5402. The detection mechanism involves checking for the presence of the string "c|3A 5C|" within the TCP packet payload. This string is a characteristic marker used by the Back Construction 2.1 backdoor during communication.

Indicators of Compromise (IoCs):

TCP Ports: 5401, 5402

Content Pattern: "c|3A 5C|"

Detection Mechanism: This rule identifies potential Back Construction 2.1 backdoor activity using the following conditions:

The network protocol must be TCP.

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

The source port must be either 5401 or 5402.

The TCP connection must be established (established).

The payload must contain the string "c|3A 5C|".

Possible Attribution & Use Cases:

This rule is useful for monitoring network traffic for malicious activity related to backdoor software.

Recommended Actions:

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

Remediation: Remove the Back Construction 2.1 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

Classtype: misc-activity

Rule SID: 152

Rule Revision: 11