Threat Category:

Malware

Backdoor

Trojan

Threat Description: The SNORT rule is designed to detect the presence of the Satan's Backdoor 2.0 Beta. This rule focuses on traffic from an internal network to an external network on TCP port 666. The detection mechanism involves checking for specific strings within the TCP packet payload. Specifically, it checks for "Remote|3A| " at a depth of 11 (case-insensitive) and "You are connected to me.|0D 0A|Remote|3A| Ready for commands" (case-insensitive) with a distance of 0. These patterns are indicative of communication from a system infected with the Satan's Backdoor.

Indicators of Compromise (IoCs):

TCP Port: 666

Content Pattern 1: "Remote|3A| " (depth 11, case-insensitive)

Content Pattern 2: "You are connected to me.|0D 0A|Remote|3A| Ready for commands" (distance 0, case-insensitive)

Detection Mechanism: This rule identifies potential Satan's Backdoor 2.0 Beta 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 666.

The TCP connection must be established (established).

The payload must contain the specified content patterns.

Possible Attribution & Use Cases:

Recommended Actions:

Monitor and Investigate: If this rule is triggered, investigate the affected systems to confirm the presence of the Satan's Backdoor.

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

Rule Author: Community

Rule Source: Community

Reference: www.megasecurity.org/trojans/s/satanzbackdoor/SBD2.0b.html, www3.ca.com/securityadvisor/pest/pest.aspx?id=5260

Rule SID: 118

Rule Revision: 12