Threat Category:

Malware

Backdoor

Trojan

Threat Description: The SNORT rule is designed to detect attempts to use the NetBus backdoor to gather information from a system. This rule focuses on traffic from an external network to an internal network on TCP ports 12345 and 12346. The detection mechanism involves checking for the presence of the string "GetInfo|0D|" within the TCP packet payload. This string is a command used by NetBus to retrieve system information.

Indicators of Compromise (IoCs):

TCP Ports: 12345, 12346

Content Pattern: "GetInfo|0D|"

Rule SID: 110

Rule Revision: 10

Detection Mechanism: This rule identifies potential NetBus GetInfo commands using the following conditions:

The network protocol must be TCP.

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

The destination ports must be either 12345 or 12346.

The TCP connection must be established (established).

The payload must contain the string "GetInfo|0D|".

Possible Attribution & Use Cases:

The detection can be used to identify attempts to use the NetBus backdoor for reconnaissance

purposes.

This rule is useful for monitoring network traffic for malicious activity related to remote administration tools.

Recommended Actions:

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

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