Threat Category: Malware, Backdoor Trojan

Threat Description: The SNORT rule is designed to detect network traffic indicative of a NetBus Pro 2.0 connection. This rule focuses on traffic from an internal network to an external network over TCP port 20034. The detection mechanism involves checking for specific content patterns within the TCP packet payload. Specifically, it looks for "BN|10 00 02 00|" at a depth of 6 bytes and "|05 00|" at a depth of 2 bytes with an offset of 8 bytes. These patterns are characteristic of the NetBus Pro 2.0 communication protocol and indicate that a connection has been established. The rule also uses the flowbits keyword to track the connection state.

Indicators of Compromise (IoCs):

TCP Port: 20034

Content Pattern 1: "BN|10 00 02 00|" (at depth 6)

Content Pattern 2: "|05 00|" (at depth 2, offset 8)

Detection Mechanism: This rule identifies potential NetBus Pro 2.0 connections 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 20034.

The TCP connection must be established (established).

The flowbits keyword is used to ensure that the rule checks for these patterns after a "backdoor.netbus_2.connect" flowbit has been set.

The payload must contain the content pattern "BN|10 00 02 00|" at a depth of 6 bytes.

The payload must also contain the content pattern "|05 00|" at a depth of 2 bytes with an offset of 8 bytes.

Recommended Actions:

Monitor and Investigate: If this rule is triggered, investigate the affected systems to confirm the presence of the NetBus Pro 2.0 backdoor.

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

Remediation: Remove the NetBus Pro 2.0 backdoor from infected systems and secure any compromised accounts.

Rule Author: Community

Rule Source: Community

Rule SID: 115

Rule Revision: 15