Threat Category: Network Traffic, POP3 Protocol

Threat Description: The SNORT rule is designed to detect POP3 connection attempts. POP3 is an application-layer internet standard protocol used by local email clients to retrieve email from a remote server over a TCP/IP connection. Detecting POP3 connections can be useful for monitoring email retrieval activity.

Indicators of Compromise (IoCs)

Protocol: TCP

Destination Port: 110

Detection Mechanism: This rule identifies POP3 connection attempts by monitoring for TCP traffic destined for port 110.

Recommended Actions:

Monitor and Investigate: Analyze POP3 traffic for suspicious login attempts or unusual activity.

Secure Alternatives: Encourage the use of more secure email retrieval protocols such as IMAP or secure POP3.

Authentication: Enforce strong authentication mechanisms.

Author & Attribution:

SID: 1000008

Revision: 1