Threat Category: Network Traffic, IMAP Protocol

Threat Description: The rule is designed to detect IMAP connection attempts. IMAP is an internet standard protocol used by email clients to access email on a remote mail server. Detecting IMAP connections is important for monitoring email access and identifying potential security risks.

Indicators of Compromise (IoCs)

Protocol: TCP

Destination Port: 143

Detection Mechanism: This rule identifies IMAP connection attempts by monitoring for TCP traffic destined for port 143.

Possible Attribution & Use Cases:

Monitoring email access activity.

Detecting potential unauthorized access to email accounts.

Troubleshooting email access issues.

Recommended Actions:

Secure Alternatives: Encourage the use of secure IMAP (IMAPS) which encrypts the communication.

Authentication: Enforce strong authentication mechanisms, such as multi-factor authentication.

Author & Attribution:

SID: 1000009

Revision: 1