Threat Category: Network Traffic, FTP Protocol

Threat Description: The SNORT rule rule5_e.txt is designed to detect FTP (File Transfer Protocol) connection attempts. FTP is a standard network protocol used for the transfer of computer files between a client and server on a computer network. Detecting FTP connections can be important for monitoring file transfers and identifying potential security risks associated with unauthorized file access.

Indicators of Compromise (IoCs)

Protocol: TCP

Destination Port: 21

Detection Mechanism: This rule identifies FTP connection attempts by monitoring for TCP traffic destined for port 21.

Possible Attribution & Use Cases:

Monitoring file transfers across the network.

Detecting unauthorized FTP access.

Troubleshooting FTP connectivity issues.

Recommended Actions:

Monitor and Investigate: Analyze FTP traffic for suspicious file transfers or unauthorized access attempts.

Secure FTP Alternatives: Encourage the use of more secure file transfer protocols such as SFTP (SSH File Transfer Protocol) or FTPS (FTP Secure).

Firewall Rules: Implement strict firewall rules to control and restrict FTP traffic.

Author & Attribution:

SID: 1000005

Revision: 1