Threat Category: Network Traffic, HTTPS Protocol

Threat Description: The SNORT rule is designed to detect HTTPS traffic. HTTPS (Hypertext Transfer Protocol Secure) is the secure version of HTTP, used for encrypted communication over the web. Detecting HTTPS traffic is crucial for monitoring secure web activity and identifying potential security risks.

Indicators of Compromise (IoCs)

Protocol: TCP

Destination Port: 443

Detection Mechanism:

Recommended Actions:

Monitor and Investigate: Analyze HTTPS traffic for suspicious patterns or anomalies.

SSL Inspection: Implement SSL inspection to decrypt and inspect HTTPS traffic for malicious content (note: this has privacy implications and should be done carefully).

Intrusion Detection: Use IDS to analyze decrypted HTTPS traffic for signs of attacks.

Author & Attribution:

SID: 1000004

Revision: 1