Threat Category: Exploit ? Remote Code Execution (RCE)

Threat Description: This detection targets exploitation attempts against SaltStack Salt servers vulnerable to CVE-2020-16846. Attackers exploit the Salt API by sending crafted HTTP POST requests to the /run endpoint with Content-Type: application/json, aiming to execute arbitrary commands remotely.

Indicators of Compromise (IoCs):

Protocol: TCP

Traffic Direction: $EXTERNAL_NET ? $HOME_NET

Destination Port: 4505

Payload Indicators:

HTTP Method: POST

HTTP URI Path: /run

HTTP Header Content-Type: application/json

Detection Mechanism:

TCP connection must be established and flowing to the server.

HTTP traffic must contain:

Method POST

URI path /run

Header with application/json

Focus is on inbound API exploitation attempts towards SaltStack server ports.

Reference:

CVE Identifier: CVE-2020-16846

Classification: Attempted-admin

Rule Metadata:

SID: 2060514

Revision: 1