Detection Strategy for Resource Hijacking: SMS Pumping via SaaS Application Logs, Detection Strategy DET0156

Archived: 2026-04-05 18:08:41 UTC

AN0443

Automated and repetitive triggering of SMS messages through OTP/account verification fields on SaaS platforms, leveraging background messaging APIs such as Twilio, AWS SNS, or Amazon Cognito to generate traffic toward attacker-controlled numbers.

Log Sources

Data Component	Name	Channel
Application Log Content (DC0038)	saas:application	High-frequency invocation of SMS-related API endpoints from publicly accessible OTP or verification forms (e.g., Twilio: SendMessage, Cognito: AdminCreateUser) with irregular destination patterns.
User Account Authentication (DC0002)	saas:audit	Repeated requests to SMS-generating endpoints using anomalous or new user agents, IP ranges, or geographies.

Mutable Elements

Field	Description
TimeWindow	Defines the rolling window over which SMS API invocation frequency is measured. Tunable based on average platform traffic.
SMSFrequencyThreshold	Number of SMS requests per endpoint or per user that should trigger investigation. Should align with business logic and user behavior.
DestinationCountryCodeFilter	Monitors if requests target known high-risk, revenue-sharing regions. Tunable to reflect SMS tariff rates or abuse history.
UserAgentAnomalyThreshold	Defines outlier score or list of unknown/automated user agents submitting forms.
IPGeoVarianceScore	Tracks abnormal geographic spread of traffic sourcing OTP triggers.

Source: https://attack.mitre.org/detectionstrategies/DET0156