Securing Cloud Integrations:

How a SaaS Firm Prevented a Novel Ransomware Attack

Overview

A SaaS company faced a sophisticated ransomware threat hidden in a phony AWS npm package, capable of encrypting production data. Veracode blocked the attack at the registry level and flagged the risk, preventing disruption and enabling secure, rapid recovery.

Problem

- SaaS cloud provider dependent on open-source AWS npm integrations.
- Attacker published a malicious package using image-based C2 to evade scans.
- Threat posed risk of widespread ransomware encryption and costly recovery.

How We Solved It

- Package Firewall enforced registry-level blocking before the malicious code could be downloaded.
- Malicious package protection capabilities automatically quarantined the payload and assigned a contextual risk score.
- Veracode SCA flagged related dependencies, recommended hardened versions, and automated safe upgrades.

Result

- **Ransomware attack fully prevented with no disruption to production.**
- **Operations restored rapidly; security posture and policies improved to stop future novel threats.**

Background

A SaaS cloud storage firm utilized npm packages that wrapped the AWS SDK to accelerate its cloud migration projects. The development team considered packages branded with familiar names like AWS to be low-risk, which led them to adopt new open-source tools quickly to maintain project momentum and speed up integration tasks.

The Incident

An attacker published a malicious package masquerading as a legitimate AWS tool. This package employed an innovative delivery tactic, hiding command-and-control (C2) instructions within a JPEG image file to evade traditional code scanning. Once installed, the package was designed to activate post-install, inject ransomware into the production environment, and encrypt critical company data.

The Impact

A successful attack would have led to widespread data encryption, forcing a difficult choice between paying a ransom or attempting a lengthy and costly recovery. The incident would have also triggered significant regulatory penalties for data loss, caused severe service disruptions for customers, and resulted in the loss of key business partners.

Resolution with Veracode

Veracode's platform provided proactive, multi-layered defense that stopped the attack at the source. Through registry-level enforcement, Veracode Package Firewall blocked the malicious package from being downloaded by using policy rules that flagged associated malicious indicators, including suspicious domains and known payload patterns. Veracode's malicious package protection capabilities validated the package against its database of emerging threat intelligence, automatically quarantining the payload and providing a contextual risk score with clear remediation steps. In parallel, Veracode SCA identified related libraries sharing similar indicators, recommended hardened versions, and automated pull requests to ensure dependencies aligned with security policy baselines.

Outcome

This pre-download prevention allowed the firm to avoid the ransomware attack entirely, restore normal operations swiftly, and harden its security policies to prevent future recurrence. Veracode SCA reinforced long-term resilience by continuously monitoring dependencies, ensuring policy compliance, and reducing the risk of similar threats resurfacing.

Key Takeaway

To defend against novel delivery tactics that evade basic scans, you need upstream controls and real-time intelligence to block packages associated with malicious indicators, reducing ransomware risk across your cloud supply chain.