TLP WHITE // [CS-TR-24-0903] Threat Actor Update Rhysida Overview

Rhysida is a rapidly emerging ransomware-as-a-service (RaaS) operation that targets critical infrastructure sectors such as healthcare, government, and logistics. Their attacks involve double extortion, where they encrypt data and threaten to leak it if the ransom is not paid, causing both financial and reputational damage. In September 2024, Rhysida launched a major attack on the Port of Seattle, disrupting operations and global supply chains. Their tactics include spear-phishing, exploiting vulnerabilities, and disabling security systems to infiltrate and lock down networks. This rising threat highlights the need for organizations to strengthen defenses, especially around phishing and patch management.

This report contains valuable insights for navigating the evolving cyber landscape. To unlock the full content, reach out to your customer success manager or email info@criticalstart.com.

CRITICALSTART® offers a pioneering solution to modern organizational challenges in aligning cyber protection with risk appetite through its Cyber Operations Risk & Response™ platform, award-winning Managed Detection and Response (MDR) services, and a dedicated human-led risk and security team. By providing continuous monitoring, mitigation, maturity assessments, and comprehensive threat intelligence research, they enable businesses to proactively protect critical assets with measurable ROI. Critical Start's comprehensive approach allows organizations to achieve the highest level of cyber risk reduction for every dollar invested, aligning with their desired levels of risk tolerance.