TLP WHITE // [CS-TR-24-0902] Chinese Cyber Threat Operations: A Comprehensive Overview

Chinese state and non-state threat actors are notorious for their advanced persistent threat (APT) tactics, techniques, and procedures (TTPs). They employ these sophisticated TTPs in their cyber espionage and disruption operations to advance their political, economic, and technological agenda. Chinese cyber threat actors frequently collaborate with one another and different malware groups, sharing tools, techniques, and even dividing the proceeds from their coordinated operations. In the past six months, Chinese threat actors have significantly escalated their cyber operations which have led to system intrusions, disruptions, and data exfiltration. In February 2024, Dutch authorities reported that Chinese state hackers exploited the CVE-2022-42475 vulnerability to deploy a remote access trojan (RAT) named CoatHanger, which serves as a backdoor. To date, the threat actors have compromised approximately 20,000 Fortinet VPN appliances. Combatting these evolving cyber threats requires a holistic approach that integrates strong cybersecurity practices with diplomatic efforts and law enforcement collaboration, ensuring a coordinated and comprehensive defense.

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.