Amaranth-Dragon Espionage Targeting Southeast Asia Exposed

By rohann@checkpoint.com

Published: 2026-02-04 · Archived: 2026-04-10 02:00:16 UTC

Executive Summary

- Check Point Research uncovered highly targeted cyber espionage campaigns aimed at government and law enforcement agencies across the ASEAN region throughout 2025.
- The activity is attributed to Amaranth-Dragon, a previously untracked threat actor assessed to be closely linked to the China-affiliated APT 41 ecosystem.
- The group weaponized newly disclosed vulnerabilities within days, including a critical WinRAR flaw, and paired them with lures tied to real-world political and security events.
- These operations demonstrate state-level discipline and precision, using country-restricted infrastructure, trusted cloud services, and stealthy tooling to quietly collect intelligence.

A New Cyber Espionage Campaign Unfolds in Southeast Asia

Throughout 2025, Check Point Research observed a series of cyber espionage campaigns quietly unfolding across Southeast Asia. Unlike opportunistic cyber crime, these operations were narrowly focused on government institutions and law enforcement agencies, suggesting a clear objective: long-term geopolitical intelligence collection.

Many of the campaigns were timed to coincide with sensitive local political developments, official government decisions, or regional security events. By anchoring malicious activity in familiar, timely contexts, the attackers significantly increased the likelihood that targets would engage with the content.

Our analysis attributes these campaigns to Amaranth-Dragon, a threat group not previously documented publicly. Tooling and operational patterns show strong similarities to APT-41, one of the most active and capable Chinese-affiliated cyber espionage groups, suggesting shared resources, knowledge, or direct affiliation.

The campaigns were designed to be highly controlled. Attack infrastructure was configured to interact only with victims in specific target countries, limiting exposure beyond intended targets. Once access was established, attackers deployed tools commonly used in legitimate security testing, repurposed here to maintain persistent access.

Exploiting Speed: Turning Disclosure Into Opportunity

A critical moment in Amaranth-Dragon’s activity came with the disclosure of CVE-2025-8088, a vulnerability affecting the popular WinRAR compression utility. Within days of public disclosure and shortly after exploit, code appeared online. The group had already incorporated the vulnerability into live campaigns. The speed and

confidence with which this vulnerability was operationalized underscores the group's technical maturity and preparedness.

Campaigns Built Around Countries, Not Volume

Amaranth-Dragon campaigns

Since March 2025, Check Point Research has tracked multiple Amaranth-Dragon campaigns targeting Cambodia, Thailand, Laos, Indonesia, Singapore, and the Philippines. Each operation was tightly scoped, typically focusing on just one or two countries at a time.

Rather than relying on mass distribution, the attackers tailored their lures to local political, economic, or military developments, such as government salary announcements or joint regional exercises. While the exact delivery channel could not be conclusively confirmed, the highly targeted nature of the campaigns strongly suggests the use of phishing emails sent directly to intended victims. Malicious archive files were often hosted on well-known cloud platforms, lending an air of legitimacy and reducing suspicion.

A standout characteristic of these campaigns was strict geographic enforcement. The attackers' infrastructure actively rejected connections from outside the intended target countries, limiting exposure and complicating external investigation. This level of control is rarely seen in criminal operations and is strongly associated with state-aligned espionage.

Over time, the campaigns evolved in sophistication, culminating in late-2025 operations targeting the Philippine government and maritime agencies, carefully timed around official national events.

Attribution: A Clear Line to APT-41

Multiple technical and operational indicators link Amaranth-Dragon to APT-41, a long-running China-linked cyber espionage group known for targeting governments worldwide.

Both groups share a focus on Southeast Asian government and law enforcement entities, as well as similar approaches to tool development and campaign execution. Patterns in infrastructure management, operational timing, and development practices point to a well-resourced team operating within the UTC+8 time zone.

Taken together, these overlaps strongly suggest that Amaranth-Dragon is either closely affiliated with or operating as part of the broader APT-41 ecosystem, extending established espionage efforts in the region under a new operational identity.

What This Means for Defenders

These campaigns underscore how modern cyber espionage combines speed, precision, and geopolitical intent. Vulnerabilities can be weaponized within days of disclosure, and carefully tailored phishing attacks can bypass traditional perimeter defenses. For government agencies and organizations in sensitive sectors, this highlights the importance of rapid patching, strong visibility into file-based threats, and layered security across both endpoints and communication channels.

Check Point Harmony Endpoint and Harmony Email & Collaboration support these efforts by helping organizations reduce exposure to targeted, file-based attacks like those observed in this activity.

Read the Full Research Report

This blog highlights key findings from an ongoing investigation. For full technical details, campaign timelines, and indicators of compromise, read the complete Check Point Research report here.
