Top Security Incidents of 2025: The Emergence of the ChainedShark APT Group - NSFOCUS, Inc., a global network and cyber security leader, protects enterprises and carriers from advanced cyber attacks.

By NSFOCUS

Published: 2026-02-13 · Archived: 2026-04-02 10:51:00 UTC

In 2025, NSFOCUS Fuying Lab disclosed a new APT group targeting China's scientific research sector, dubbed "ChainedShark" (tracking number: Actor240820). Been active since May 2024, the group's operations are marked by high strategic coherence and technical sophistication. Its primary targets are professionals in Chinese universities and research institutions specializing in international relations, marine technology, and related fields, with the intent to steal sensitive data and intelligence in diplomacy and marine technology.

ChainedShark exhibits clear geopolitical motivations, focusing its attacks on experts and scholars in international relations and marine sciences within Chinese academic and research institutions. The group demonstrates strong social engineering capabilities, crafting fluent, natural, and high-quality Chinese-language lures. It skillfully exploits professional scenarios—such as conference invitations and academic call-for-papers—to create deceptive attack vectors, effectively lowering targets' guard.

Technically, ChainedShark operates at the level of a state-sponsored attack team. Its arsenal integrates N-day vulnerability exploits and highly complex custom trojans, featuring meticulously designed attack chains and

payloads with strong evasion and stealth capabilities. This indicates a mature attack infrastructure and continuous weapon development capacity.

Event Summary

ChainedShark's attack campaigns, while maintaining consistent strategic objectives, have demonstrated a clear evolutionary trajectory in both tactics and technical execution.

First Wave (May 2024): This initial attack remains the most complex operation identified to date. The attack chain deployed a custom-developed trojan, LinkedShell, characterized by high customization and advanced anti-forensic capabilities. The technical intricacies of this trojan underscore the group's robust initial weaponization capabilities.

Subsequent Attacks (August–November 2024): In later operations, the attackers adjusted their tactics. By successfully exploiting the GrimResource vulnerability (publicly disclosed in June 2024), they significantly streamlined the attack process, reflecting a strategic shift toward leveraging public vulnerabilities to enhance efficiency and cost-effectiveness.

Event Analysis

Multidimensional clue correlation linked separate attack events across different timeframes, painting a comprehensive profile of the threat actor.

- Target Consistency: The same individuals were targeted in both the May and November 2024 attacks, strongly indicating the directed and persistent nature of these operations.
- Lure Homogeneity: Despite variations in payloads, the phishing emails used in different attacks shared striking similarities in subject selection, phrasing, and social engineering tactics—forming a behavioral "fingerprint."

This correlational analysis not only provides critical evidence for attribution but also reveals that ChainedShark adheres to a mature social engineering script and attack management process throughout its prolonged campaigns.
