APT 30, Override Panda - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:13:04 UTC

DescriptionAPT 30 is a threat group suspected to be associated with the Chinese government. While Naikon, Lotus Panda shares some characteristics with APT 30, the two groups do not appear to be exact matches.

(FireEye) When our Singapore-based FireEye labs team examined malware aimed predominantly at entities in Southeast Asia and India, we suspected that we were peering into a regionally focused cyber espionage operation. The malware revealed a decade-long operation focused on targets—government and commercial—who hold key political, economic, and military information about the region. This group, who we call APT30, stands out not only for their sustained activity and regional focus, but also for their continued success despite maintaining relatively consistent tools, tactics, and infrastructure since at least 2005.

Based on our knowledge of APT30's targeting activity and tools, their objective appears to be data theft as opposed to financial gain. APT30 has not been observed to target victims or data that can be readily monetized (for example, credit card data, personally identifiable information, or bank transfer credentials). Instead, their tools include functionality that allows them to identify and steal documents, including what appears to be an interest in documents that may be stored on air-gapped networks.

The group expresses a distinct interest in organizations and governments associated with ASEAN, particularly so around the time of official ASEAN meetings.

Many of APT30's decoy documents use topics related to Southeast Asia, India, border areas, and broader security and diplomatic issues. Decoy documents attached to spear phishing emails are frequently indicators of intended targeting because threat actors generally tailor these emails to entice their intended targets —who typically work on related issues—to click on the attachments and infect themselves.

In addition to APT30's Southeast Asia and India focus, we've observed APT30 target journalists reporting on issues traditionally considered to be focal points for the Chinese Communist Party's sense of legitimacy, such as corruption, the economy, and human rights. In China, the Communist Party has the ultimate authority over the government. China-based threat groups have targeted journalists before; we believe they often do so to get a better understanding on developing stories to anticipate unfavorable coverage and better position themselves to shape public messaging.
