Aoqin Dragon - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:52:24 UTC

APT group: Aoqin Dragon

Names	Aoqin Dragon *(SentinelLabs)* UNC94 *(Mandiant)* G1007 *(MITRE)*
Country	China
Motivation	Information theft and espionage
First seen	2013
Description	(SentinelLabs) SentinelLabs has uncovered a cluster of activity beginning at least as far back as 2013 and continuing to the present day, primarily targeting organizations in Southeast Asia and Australia. We assess that the threat actor's primary focus is espionage and relates to targets in Australia, Cambodia, Hong Kong, Singapore, and Vietnam. We track this activity as 'Aoqin Dragon'. The threat actor has a history of using document lures with pornographic themes to infect users and makes heavy use of USB shortcut techniques to spread the malware and infect additional targets. Attacks attributable to Aoqin Dragon typically drop one of two backdoors, Mongall and a modified version of the open source Heyoka project.
Observed	Sectors: Education, Government, Telecommunications. Countries: Australia, Cambodia, Hong Kong, Singapore, Vietnam.
Tools used	Mongall.
Information	<https://www.sentinelone.com/labs/aoqin-dragon-newly-discovered-chinese-linked-apt-has-been-quietly-spying-on-organizations-for-10-years/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G1007/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format