Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:37:13 UTC

APT group: Moafee

Names	Moafee *(FireEye)* G0002 *(MITRE)*
Country	China
Motivation	Information theft and espionage
First seen	2014
Description	Moafee is a threat group that appears to operate from the Guandong Province of China. Due to overlapping TTPs, including similar custom tools, Moafee is thought to have a direct or indirect relationship with the threat group DragonOK. (FireEye) The attack group “Moafee” (named after their command and control infrastructure) appears to operate out of the Guangdong province in China and is known to target the governments and military organizations of countries with national interests in the South China Sea. The seas in this region have multiple claims of sovereignty and hold high significance, as it is the second busiest sea-lane in the world and are known to be rich in resources such as rare earth metals, crude oil, and natural gas. We have also observed the Moafee group target organizations within the US defense industrial base.
Observed	Sectors: Defense, Government. Countries: USA and “countries with national interests in the South China Sea”.
Tools used	HTran, Mongall, NewCT2, NFlog, Poison Ivy.
Information	<https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0002/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format