Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:53:44 UTC

APT group: Lancefly

Names	Lancefly *(Symantec)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2018
Description	(Symantec) The Lancefly advanced persistent threat (APT) group is using a custom-written backdoor in attacks targeting organizations in South and Southeast Asia, in activity that has been ongoing for several years. Lancefly may have some links to previously known groups, but these are low confidence, which led researchers at Symantec, by Broadcom Software, to classify this activity under a new group name. Lancefly's custom malware, which we have dubbed Merdoor, is a powerful backdoor that appears to have existed since 2018. Symantec researchers observed it being used in some activity in 2020 and 2021, as well as this more recent campaign, which continued into the first quarter of 2023. The motivation behind both these campaigns is believed to be intelligence gathering.
Observed	Sectors: Aviation, Education, Government, Telecommunications. Countries: South and Southeast Asia.
Tools used	Merdoor.
Information	<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lancefly-merdoor-zxshell-custom-backdoor>

Last change to this card: 21 June 2023

Download this actor card in PDF or JSON format