

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:15:05 UTC

APT group: TA2722

Names	TA2722 (<i>Proofpoint</i>) Balikbayan Foxes (<i>Proofpoint</i>)
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2020
Description	<p>(Proofpoint) Proofpoint identified a new and highly active cybercriminal threat actor, TA2722, colloquially referred to by Proofpoint threat researchers as the Balikbayan Foxes. Throughout 2021, a series of campaigns impersonated multiple Philippine government entities including the Department of Health, the Philippine Overseas Employment Administration (POEA), and the Bureau of Customs. Other related campaigns masqueraded as the Manila embassy for the Kingdom of Saudi Arabia (KSA) and DHL Philippines. The messages were intended for a variety of industries in North America, Europe, and Southeast Asia, with the top sectors including Shipping, Logistics, Manufacturing, Business Services, Pharmaceutical, Energy, and Finance.</p>
Observed	Sectors: Energy , Financial , Manufacturing , Pharmaceutical , Shipping and Logistics . Countries: USA and Europe and Southeast Asia.
Tools used	NanoCore RAT , RemcosRAT .
Information	< https://www.proofpoint.com/us/blog/threat-insight/new-threat-actor-spoofs-philippine-government-covid-19-health-data-widespread >

Last change to this card: 04 November 2021

Download this actor card in [PDF](#) or [JSON](#) format

Source: <https://apt.etda.or.th/cgi-bin/showcard.cgi?u=6b9f8bf4-afdf-4ff4-bc59-9dc4f9dea767>