

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:02:02 UTC

APT group: TA2541

Names	TA2541 (<i>Proofpoint</i>)
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2017
Description	(Proofpoint) TA2541 is a persistent cybercriminal actor that distributes various remote access trojans (RATs) targeting the aviation, aerospace, transportation, and defense industries, among others. Proofpoint has tracked this threat actor since 2017, and it has used consistent tactics, techniques, and procedures (TTPs) in that time. Entities in the targeted sectors should be aware of the actor's TTPs and use the information provided for hunting and detection.
Observed	Sectors: Aviation , Aerospace , Defense , Transportation .
Tools used	Agent Tesla , AsyncRAT , Ave Maria , DarkRAT , H-Worm , Imminent Monitor RAT , Luminosity RAT , NetWire RC , Parallax RAT , RevengeRAT .
Information	< https://www.proofpoint.com/us/blog/threat-insight/charting-ta2541s-flight >

Last change to this card: 03 April 2022

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

Source: <https://apt.etda.or.th/cgi-bin/showcard.cgi?u=c830c769-f4d2-4c55-a77b-14632333e7d2>