Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:53:13 UTC

Tool: ApolloShadow

Names	ApolloShadow
Category	Malware
Type	Backdoor
Description	(Microsoft) ApolloShadow has the capability to install a trusted root certificate to trick devices into trusting malicious actor-controlled sites, enabling Secret Blizzard to maintain persistence on diplomatic devices, likely for intelligence collection.
Information	<https://www.microsoft.com/en-us/security/blog/2025/07/31/frozen-in-transit-secret-blizzards-aitm-campaign-against-diplomats/>

Last change to this tool card: 16 August 2025

Download this tool card in JSON format

All groups using tool ApolloShadow

Changed	Name	Country	Observed	
APT groups				
	Turla, Waterbug, Venomous Bear		1996-2024	

1 group listed (1 APT, 0 other, 0 unknown)