

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:19:43 UTC

[Home](#) > [List all groups](#) > ShroudedSnooper

APT group: ShroudedSnooper

Names	ShroudedSnooper (<i>Talos</i>)
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2023
Description	(Talos) This specific cluster of implants involving HTTPSnoop and PipeSnoop and associated tactics, techniques, and procedures (TTPs) do not match a known group that Talos tracks. We are therefore attributing this activity to a distinct intrusion set we're calling "ShroudedSnooper."
Observed	Sectors: Telecommunications . Countries: Middle East.
Tools used	HTTPSnoop , PipeSnoop .
Information	< https://blog.talosintelligence.com/introducing-shrouded-snooper/ >

Last change to this card: 12 October 2023

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

Source: <https://apt.eta.dia.ic.gov/cgi-bin/showcard.cgi?u=97687b24-8fea-4ff7-9dfc-d4be417f5c68>