Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:48:50 UTC

APT group: Indra

Names	Indra *(self given)*
Country	[Unknown]
Motivation	Sabotage and destruction
First seen	2019
Description	(Check Point) Check Point Research (CPR) warns governments everywhere of the importance of protecting critical infrastructure, as it learns that the July 9 cyber attack on Iran's train system was carried out by Indra, a group that identifies itself as regime opposition and has the capability to wipe out data without direct means for recovery. • CPR analyzed artifacts left by the July 9 cyber attack on Iran's train system, attributing the attacks to a group that self-identifies as Indra • CPR confirms that Indra was also responsible for cyber attacks against multiple companies in Syria in 2019 and 2020 • CPR cites cyber attack on Iran's train system as an example for governments around the world of how a single group can create disruption on critical infrastructure
Observed	Sectors: Energy, Transportation. Countries: Iran, Syria.
Tools used	Comet.
Information	<https://blog.checkpoint.com/2021/08/14/indra-group-attack-on-iran-highlights-the-threats-to-global-critical-infrastructure/> <https://research.checkpoint.com/2021/indra-hackers-behind-recent-attacks-on-iran/>

Last change to this card: 01 November 2021

Download this actor card in PDF or JSON format
