Operation Tainted Love - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:21:08 UTC

APT group: Operation Tainted Love

Names	Operation Tainted Love *(SentinelLabs)*
Country	China
Motivation	Information theft and espionage
First seen	2023
Description	(SentinelLabs) In Q1 of 2023, SentinelLabs observed initial phases of attacks against telecommunication providers in the Middle East. We assess that this activity represents an evolution of tooling associated with Operation Soft Cell. While it is highly likely that the threat actor is a Chinese cyberespionage group in the nexus of Gallium and APT 41, the exact grouping remains unclear. SentinelLabs observed the use of a well-maintained, versioned credential theft capability and a new dropper mechanism indicative of an ongoing development effort by a highly-motivated threat actor with specific tasking requirements.
Observed	Sectors: Telecommunications. Countries: Middle East.
Tools used	mim221, Mimikatz.
Information	<https://www.sentinelone.com/labs/operation-tainted-love-chinese-apts-target-telcos-in-new-attacks/>

Last change to this card: 27 December 2024

Download this actor card in PDF or JSON format