Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:48:58 UTC

APT group: Sandman

Names	Sandman *(SentinelLabs)*
Country	China
Motivation	Information theft and espionage
First seen	2022
Description	(SentinelLabs) In collaboration with QGroup GmbH, SentinelLabs observed over August 2023 a threat activity cluster targeting the telecommunication sector. The activities have been conducted by a threat actor of unknown origin using a novel modular backdoor based on the LuaJIT platform. We dub this threat actor and the backdoor Sandman and LuaDream in reference to what we suspect to be the backdoor's internal name – DreamLand client. The activities we observed are characterized by strategic lateral movement to specific targeted workstations and minimal engagement, suggesting a deliberate approach aimed at achieving the set objectives while minimizing the risk of detection.
Observed	Sectors: Telecommunications. Countries: Middle East, Western Europe, and South Asia.
Tools used	LuaDream.
Information	<https://www.sentinelone.com/labs/sandman-apt-a-mystery-group-targeting-telcos-with-a-luajit-toolkit/> <https://www.sentinelone.com/labs/sandman-apt-china-based-adversaries-embrace-lua/>

Last change to this card: 16 January 2024

Download this actor card in PDF or JSON format
