Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:08:00 UTC

Tool: GOLDBACKDOOR

Names	GOLDBACKDOOR
Category	Malware
Type	Backdoor
Description	(Stairwell) Stairwell assesses with medium-high confidence that GOLDBACKDOOR is the successor of, or used in parallel with, the malware BLUELIGHT, attributed to APT37 / Ricochet Chollima. This assessment is based on technical overlaps between the two malware families and the impersonation of NK News, a South Korean news site focused on the DPRK.
Information	<https://stairwell.com/news/threat-research-the-ink-stained-trail-of-goldbackdoor/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.goldbackdoor>

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool GOLDBACKDOOR

Changed	Name	Country	Observed	
APT groups				
	Reaper, APT 37, Ricochet Chollima, ScarCruft		2012-Mar 2025	

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