Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:47:39 UTC

Tool: LIGHTRAIL

Names	LIGHTRAIL
Category	Malware
Type	Tunneling
Description	(Mandiant) LIGHTRAIL has several connections to MINIBIKE and MINIBUS in the form of (1) a shared code base, (2) Azure C2 infrastructure with similar patterns and naming, and (3) overlapping targets and victimology. LIGHTRAIL communicates with an Azure C2 subdomain of the form *[.]* [.]cloudapp[.]azure[.]com. Mandiant assesses with medium confidence that both LIGHTRAIL and MINIBIKE were used to target the same victim environment at least once.
Information	<https://cloud.google.com/blog/topics/threat-intelligence/suspected-iranian-unc1549-targets-israel-middle-east>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.lightrail>

Last change to this tool card: 29 December 2024

Download this tool card in JSON format

All groups using tool LIGHTRAIL

Changed	Name	Country	Observed	
APT groups				
	↳ Subgroup: TA455, Smoke Sandstorm		2021-Sep 2023	

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