

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:53:10 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool CordScan

Tool: CordScan

Names	CordScan
Category	Malware
Type	Reconnaissance
Description	(CrowdStrike) This executable is a network scanning and packet capture utility that contains built-in logic relating to the application layer of telecommunications systems, which allows for fingerprinting and the retrieval of additional data when dealing with common telecommunication protocols from infrastructure such as SGSNs. SGSNs could be targets for further collection by the adversary, as they are responsible for packet data delivery to and from mobile stations and also hold location information for registered GPRS users. CrowdStrike identified multiple versions of this utility, including a cross-compiled version for systems running on ARM architecture, such as Huawei's commercial CentOS-based operating system EulerOS.
Information	< https://www.crowdstrike.com/blog/an-analysis-of-lightbasin-telecommunications-attacks/ >

Last change to this tool card: 03 November 2021

Download this tool card in [JSON](#) format

All groups using tool CordScan

Changed	Name	Country	Observed
APT groups			
	LightBasin		2016

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