Threat Group Cards: A Threat Actor Encyclopedia

Tool: ReconShark

Names	ReconShark
Category	Malware
Type	Reconnaissance
Description	(SentinelOne) The ability of ReconShark to exfiltrate valuable information, such as deployed detection mechanisms and hardware information, indicates that ReconShark is part of a Kimsuky-orchestrated reconnaissance operation that enables subsequent precision attacks, possibly involving malware specifically tailored to evade defenses and exploit platform weaknesses.
Information	<https://www.sentinelone.com/labs/kimsuky-evolves-reconnaissance-capabilities-in-new-global-campaign/>

Last change to this tool card: 21 June 2023

Download this tool card in JSON format

All groups using tool ReconShark

Changed	Name	Country	Observed	
APT groups				
	Kimsuky, Velvet Chollima		2012-Aug 2025	

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