Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:32:15 UTC

Tool: TODDLERSHARK

Names	TODDLERSHARK
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer
Description	(Kroll) The Kroll CTI team observed a campaign using a new malware that appears to be very similar to BabyShark, previously reported to have been developed and used by the APT group Kimsuky (KTA082). The malware was deployed as part of an attempted compromise that was detected and stopped by the Kroll Responder team. The activity started with exploitation of a recently addressed authentication bypass in the remote desktop software ScreenConnect, developed by ConnectWise.
Information	<https://www.kroll.com/en/insights/publications/cyber/screenconnect-vulnerability-exploited-to-deploy-babyshark>

Last change to this tool card: 10 March 2024

Download this tool card in JSON format

All groups using tool TODDLERSHARK

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

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