Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:43:54 UTC

Tool: BabyShark

Names	BabyShark LATEOP
Category	Malware
Type	Reconnaissance, Backdoor
Description	BabyShark is Microsoft Visual Basic (VB) script-based malware family first seen in November 2018. The malware is launched by executing the first stage HTA from a remote location, thus it can be delivered via different file types including PE files as well as malicious documents. It exfiltrates system information to C2 server, maintains persistence on the system, and waits for further instruction from the operator. (Palo Alto) Based on our research, it appears the malware author calls the encoded secondary payload “Cowboy” regardless of what malware family is delivered. In our analysis, we found BabyShark attacks were using KimJongRAT and Gh0st RAT as the encoded secondary payload and thus were the “Cowboys”.
Information	<https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/> <https://unit42.paloaltonetworks.com/babyshark-malware-part-two-attacks-continue-using-kimjongrat-and-pcrat/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0414/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.babyshark>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:BabyShark>

Last change to this tool card: 30 November 2023

Download this tool card in JSON format

All groups using tool BabyShark

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

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=6740d62a-db55-4938-a560-47d7ff7a529c