Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:43:24 UTC

Tool: PowHeartBeat

Names	PowHeartBeat
Category	Malware
Type	Backdoor
Description	(ESET) PowHeartBeat is a full-featured backdoor written in PowerShell, obfuscated using various techniques such as compression, encoding, and encryption. Based on ESET telemetry, we believe PowHeartBeat replaced CLRLoad in more recent Worok campaigns as the tool used to launch PNGLoad.
Information	<https://www.welivesecurity.com/2022/09/06/worok-big-picture/>

Last change to this tool card: 13 September 2022

Download this tool card in JSON format

All groups using tool PowHeartBeat

Changed	Name	Country	Observed	
APT groups				
	Worok		2020	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ce37b5d7-a9c6-4348-a4f1-f23fb90f322c