Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:19:52 UTC

Tool: POWERPOST

Names	POWERPOST
Category	Malware
Type	Reconnaissance, Info stealer
Description	(Mandiant) POWERPOST is a reconnaissance tool written in PowerShell that can collect data on a local host including system information and user account names. POWERPOST writes the data to disk and then sends the collected data to a hardcoded remote server via HTTP POSTs.
Information	<https://www.mandiant.com/media/17826>

Last change to this tool card: 13 September 2022

Download this tool card in JSON format

All groups using tool POWERPOST

Changed	Name	Country	Observed	
APT groups				
	APT 42		2015-Feb 2024	

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