Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:44:12 UTC

Tool: ZUMKONG

Names	ZUMKONG
Category	Malware
Type	Credential stealer
Description	(FireEye) ZUMKONG is a credential stealer capable of harvesting usernames and passwords stored by Internet Explorer and Chrome browsers. Stolen credentials are emailed to the attacker via HTTP POST requests to mail[.]zmail[.]ru
Information	<https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool ZUMKONG

Changed	Name	Country	Observed	
APT groups				
	Reaper, APT 37, Ricochet Chollima, ScarCruft		2012-Mar 2025	

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