Rampant Kitten - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:50:16 UTC

APT group: Rampant Kitten

Names	Rampant Kitten *(Check Point)*
Country	Iran
Motivation	Information theft and espionage
First seen	2014
Description	(Check Point) Check Point Research unraveled an ongoing surveillance operation by Iranian entities that has been targeting Iranian expats and dissidents for years. While some individual sightings of this attack were previously reported by other researchers and journalists, our investigation allowed us to connect the different campaigns and attribute them to the same attackers. Among the different attack vectors we found were: • Four variants of Windows infostealers intended to steal the victim's personal documents as well as access to their Telegram Desktop and KeePass account information • Android backdoor that extracts two-factor authentication codes from SMS messages, records the phone's voice surroundings and more • Telegram phishing pages, distributed using fake Telegram service accounts The above tools and methods appear to be mainly used against Iranian minorities, anti-regime organizations and resistance movements such as: • Association of Families of Camp Ashraf and Liberty Residents (AFALR) • Azerbaijan National Resistance Organization • Balochistan people
Observed	Countries: Iranian minorities, anti-regime organizations and resistance movements.
Tools used	
Information	<https://research.checkpoint.com/2020/rampant-kitten-an-iranian-espionage-campaign/>

Last change to this card: 19 October 2020

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=71cc4f7d-4b04-4b1b-8947-a03dc464739d