

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:02:53 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool MPKBot



Tool: MPKBot

Names	MPKBot MPK
Category	Malware
Type	Backdoor , Info stealer
Description	(Palo Alto) We also found a second IRC bot called MPK using the same IP for its C2 server that a Leash sample was hosted on. This MPK IRC bot is very similar to the MPK Trojan that used a custom C2 communications protocol, as detailed in a whitepaper by CheckPoint regarding a threat group called Rocket Kitten. We believe this version of the MPK Trojan is based on the same code base, as both the IRC version and the one referenced in the white paper have considerable similarities from a behavior standpoint as well as direct code overlap.
Information	< https://unit42.paloaltonetworks.com/unit42-magic-hound-campaign-attacks-saudi-targets/ > < https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.mpkbot >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:MPKBot >

Last change to this tool card: 14 May 2020

Download this tool card in [JSON](#) format

All groups using tool MPKBot

Changed	Name	Country	Observed	
APT groups				
	Cutting Kitten, TG-2889		2012-Mar 2016	

	Magic Hound , APT 35 , Cobalt Illusion , Charming Kitten		2012-Jun 2025	
--	--	---	---------------	---

2 groups listed (2 APT, 0 other, 0 unknown)

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=e656fbde-296b-4a80-82fd-1676efa7b068>