

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:48:10 UTC

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

Tool: RocketMan

Names	RocketMan
Category	Malware
Type	Backdoor
Description	<p>(Kaspersky) We call this Trojan RocketMan after the string the developer uses for beaconing. Another string inside this malware is “TrumpTower”, used as an RC4 encryption initial vector.</p> <p>This malware reads the C2 IP and port from the registry where it was saved by the previous stager. It processes the following commands from its C2 that are received encrypted over HTTP:</p>
Information	< https://securelist.com/turla-renews-its-arsenal-with-topinambour/91687/ >

Last change to this tool card: 20 April 2020

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

All groups using tool RocketMan

Changed	Name	Country	Observed	
APT groups				
	Tomiris	[Unknown]	2020	
	Turla , Waterbug , Venomous Bear		1996-2024	

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