

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:46:12 UTC

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

Tool: CommonMagic

Names	CommonMagic
Category	Malware
Type	Backdoor
Description	(Kaspersky) All the victims of PowerMagic were also infected with a more complicated, previously unseen, modular malicious framework that we named CommonMagic. This framework was deployed after initial infection with the PowerShell backdoor, leading us to believe that CommonMagic is deployed via PowerMagic.
Information	< https://securelist.com/bad-magic-apt/109087/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.common_magic >

Last change to this tool card: 22 June 2023

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

All groups using tool CommonMagic

Changed	Name	Country	Observed
APT groups			
	Bad Magic , RedStinger	[Unknown]	2020-May 2023

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=60f086b5-9fb3-4c03-a8b2-5ce2862794c1>