Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 10:47:57 UTC

Tool: MuddyC2Go

Names	MuddyC2Go
Category	Malware
Type	Backdoor
Description	(Deep Instinct) While analyzing previous PhonyC2 infrastructure, Deep Instinct uncovered anomalies that indicated MuddyWater might be using an additional C2 framework. At that time, we lacked sufficient evidence to support this claim. However, after we published our PhonyC2 research, we observed two IP addresses previously related to MuddyWater, one of those addresses which was hosting PhonyC2 had switched to a different C2 framework delivering a PowerShell payload. This behavior heightened suspicions of a new C2 framework. However, without seeing and observing the initial payload, those IP addresses could have been internal tests by MuddyWater before fully deploying the C2.
Information	<https://www.deepinstinct.com/blog/muddyc2go-latest-c2-framework-used-by-iranian-apt-muddywater-spotted-in-israel>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.muddyc2go>

Last change to this tool card: 17 January 2024

Download this tool card in JSON format

All groups using tool MuddyC2Go

Changed	Name	Country	Observed	
APT groups				
	MuddyWater, Seedworm, TEMP.Zagros, Static Kitten		2017-Jul 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=84270a76-a828-4e46-a343-6ac3015f7afc