Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:05:46 UTC

Tool: Mudwater

Names	Mudwater
Category	Malware
Type	Reconnaissance, Backdoor, Exfiltration, Downloader
Description	(Trend Micro) In addition to uncovering new campaigns, we were also able to find connections between MuddyWater and four Android malware variants that posed as legitimate applications. We were able to establish proof of connection through their shared infrastructure, e.g., IP addresses and C&C servers, and the code similarities between some of the malware families. We first noticed the first Android malware variant (AndroidOS_Mudwater.HRX) when we discovered that its IP address and C&C server, 78[.]129[.]139[.]131, was used as the final C&C server of a MuddyWater campaign. In the said campaign, we saw victims receiving commands for downloading a second stage payload from the abovementioned IP address.
Information	<https://documents.trendmicro.com/assets/white_papers/wp_new_muddywater_findings_uncovered.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.mudwater>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Mudwater

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

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